VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

ÚSTAV SOUDNÍHO INŽENÝRSTVÍ

INSTITUTE OF FORENSIC ENGINEERING

PROCESNÍ FMECA - ZAVÁDĚNÍ INFORMAČNÍHO SYSTÉMU V BANCE

PROCESS FMECA - IMPLEMENTATION OF INFORMATION SYSTEM IN THE BANK

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Marie Müllerová**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Petr Blecha, Ph.D.**
SUPERVISOR

BRNO 2017

Vysoké učení technické v Brně, Ústav soudního inženýrství

Akademický rok: 2016/17

ZADÁNÍ DIPLOMOVÉ PRÁCE

student(ka): Bc. Marie Müllerová

který/která studuje v **magisterském studijním programu**

obor: **Řízení rizik firem a institucí (3901T048)**

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma diplomové práce:

Procesní FMECA - zavádění informačního systému v bance

v anglickém jazyce:

Process FMECA - implementation of information system in the bank

Stručná charakteristika problematiky úkolu:

Cílem práce je identifikovat potenciální chyby a jejich následky při procesu zavádění informačního systému v bance. Dále provést analýzu kritičnosti následků těchto chyb a navrhnout preventivní opatření vedoucí ke snížení dopadu a zvýšení efektivnosti informačního systému.

Cíle diplomové práce:

1) Proveďte rešerši využití metod FMEA a FMECA
2) Popište proces zavádění informačního systému v bance a identifikujte jeho dílčí subprocesy
3) Aplikujte metodu FMECA na proces zavádění informačního systému v bance
4) Stanovte preventivní opatření vedoucí ke snížení dopadu chyb a zvýšení efektivnosti zaváděného informačního systému

Seznam odborné literatury:

ČSN EN 60812:2007 - Techniky analýzy bezporuchovosti systémů – Postup analýzy způsobů a důsledků poruch (FMEA)
ČSN EN 61025:2007 - Analýza stromu poruchových stavů (FTA)
MAREK, J.; BLECHA, P.; MAREČEK, J.; KRČÁLOVÁ, E. Management rizik v konstrukci výrobních strojů. odborná monografie vydaná formou speciálního vydání časopisu MM Průmyslové spektrum ISSN 1212- 2572. odborná monografie vydaná formou speciálního vydání časopisu MM Průmyslové spektrum ISSN 1212- 2572. Praha: MM publishing, 2009. 90 s.

Vedoucí diplomové práce: doc. Ing. Petr Blecha, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2016/17.

V Brně, dne 21. 10. 2016

L.S.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
ÚSTAV SOUDNÍHO INŽENÝRSTVÍ
-4-

doc. Ing. Aleš Vémola, Ph.D.
ředitel vysokoškolského ústavu

Abstrakt

Tato diplomová práce se zabývá procesní FMECA analýzou, aplikovanou na proces zavádění informačního systému v bance. Teoretická část práce je zaměřena na řízení rizik a využití metod FMEA a FMECA. V praktické části je představena společnost, pro kterou je proces zavádění informačního systému navržen. Dále je provedena analýza vnějšího a vnitřního prostředí ve vztahu k informačnímu systému, z jejichž výsledků vychází SWOT matice. Poté je popsán proces zavádění informačního systému a provedena analýza FMECA. Na základě výsledků z analýzy jsou navržena vhodná opatření, která povedou k eliminaci nebezpečí nebo ke snížení jejich dopadu.

Abstract

This thesis considers of process FMECA analysis that is applied to the process of implementation the information system in the bank. The theoretical part focuses on risk management and using of methods FMEA and FMECA. In the practical part of thesis is introduced the company, for that the process of implementation of the information system is designed. In addition the analysis of the external and internal environment in relaiton to the information system is made. The result of these analysis is SWOT analysis. Then the process of implementation the information system is described and FMECA analysis is performed. Based of the results of the analysis are designed appropriate measures that will eliminate the risks or that will reduce their impacts.

Klíčová slova

Řízení rizik, analýza rizik, nebezpečí, porucha, FMEA, FMECA, informační systém.

Keywords

Risk management, risk analysis, risk, failure, FMEA, FMECA, information system.

Bibliografická citace (vzor, generuje se v IS)

MÜLLEROVÁ, M. Procesní FMECA-zavádění informačního systému v bance. Brno: Vysoké učení technické v Brně. Ústav soudního inženýrství, 2017. 90 s. Vedoucí diplomové práce doc. Ing. Petr Blecha, Ph.D.

Prohlášení

Prohlašuji, že jsem diplomovou práci zpracovala samostatně a že jsem uvedla všechny použité informační zdroje.

V Brně dne 25. května 2017

…….

podpis diplomanta

Poděkování

Na tomto místě bych chtěla poděkovat svému vedoucímu diplomové práce, panu doc. Ing. Petru Blechovi, Ph.D., a svému oponentovi, panu doc. Ing. Miloši Kochovi, CSc., za cenné rady a připomínky při zpracovávání této práce. Dále bych chtěla poděkovat společnosti Air Bank, a.s., za poskytnutí materiálů a konzultací k řešené problematice, za trpělivost a pomoc při zpracování této diplomové práce.

OBSAH

ÚVOD

Zavedení nového informačního systému je vždy náročný proces, který klade významné kapacitní nároky nejen na tým zhotovitele, ale také na zadavatele informačního systému a zejména jeho zaměstnance, kteří se implementace aktivně účastní. Společnost, která nový informační systém zavádí, může být překvapena časovou náročností zhotovením jednotlivých analýz a požadovanou součinností při řešení informačního systému. Podcenění přípravy a nespecifikování požadavků může způsobit výrazné prodražení celého projektu.

Proto je velmi důležitá spolupráce obou stran po celou dobu trvání projektu. Otázky, které by si mělo vedení společnosti položit, zní: Do jaké míry jsou současné informační technologie schopné přispět ke zvyšování růstu tržeb? Jaká je návratnost investice do nového informačního systému? Jaký podíl investic do informačních technologií doopravdy vytváří konkurenční výhodu, která je v daném oboru nová?

O přínosech nového informačního systému by se mělo uvažovat velmi konkrétně, a ještě před začátkem projektu. V opačném případě lze očekávat, že vedení společnosti bude vyčíslovat spíše ztráty, případně že proinvestované finanční prostředky nepřinesou očekávané přínosy. Pokud chybí jasný cíl, ke kterému má být směřováno vynaložené úsilí, nelze na konci cesty diskutovat o nežádoucím výsledku projektu.

Teoretická část této práce je zaměřena na oblast řízení rizik, analýzu rizik a popis metod FMEA a FMECA. V praktické části práce je představena společnost, pro kterou je provedena procesní analýza FMECA na zavádění informačního systému. Dále je provedena analýza vnějšího a vnitřního prostředí podniku ve vztahu k informačnímu systému, jejíž výstupem je výstupem je Strenghts, Weeknesses, Opportunities, Threats (dále jen SWOT) matice. Součástí praktické části práce je také popis zavádění informačního systému a provedení analýzy FMECA. Na základě výsledků z této analýzy jsou navržena vhodná opatření, která povedou ke snížení dopadu nebo ke snížení pravděpodobnosti výskytu těchto nebezpečí.

CÍL PRÁCE

Hlavním cílem této diplomové práce je provedení procesní analýza FMECA na zavedení nového informačního systému v bance, a stanovení takových opatření, která povedou ke snížení dopadu nebezpečí nebo ke snížení pravděpodobnosti jejich výskytu. Dílčím cílem je analýza vnitřního a vnějšího prostředí podniku, ze kterých bude zhotovena SWOT matice, jejíž výsledkem bude rozhodnutí, zda zavést nový informační systém, nebo ponechat stávající.

Dalším dílčím cílem je provedení detailního popisu procesu zavádění informačního systému a rozdělení tohoto procesu na jednotlivé subprocesy. Pro každý subproces budou identifikována všechna nebezpečí, jejich příčiny a následky. Dále bude zhotovena kompletní analýza FMECA a detailní návrh opatření pro ta nebezpečí, která jsou pro podnik kritická.

1 TEORETICKÁ ČÁST

Teoretická část práce obsahuje teoretická východiska, která tvoří základ pro praktickou část práce a vlastní návrhy řešení.

1.1 RIZIKO

Definice rizika je stěžejním pojmem pro řízení rizik. V nejširším slova smyslu může být riziko definováno jako „vystavení nepříznivým okolnostem“. V oblasti řízení informačních rizik se nejčastěji uvádí definice, která riziko popisuje jako možnost, že specifická hrozba využije specifické zranitelnosti systému, překoná stávající opatření, a způsobí narušení důvěrnosti, integrity nebo dostupnosti aktiva. A to povede ke vzniku škody [1] [4].

V tabulce č. 1 jsou uvedeny a vysvětleny základní pojmy související s řízením rizik.

Tabulka č. 1 - Základní pojmy [1]

Pojem	Vysvětlení
Aktivum	Vše, co má pro společnost nějakou hodnotu
Hrozba	Náhodná nebo úmyslně vyvolaná událost, která může mít negativní dopad na aktiva
Zranitelnost	Vhodnost daného aktiva umožňující uplatnění hrozby
Dopad	Následek nežádoucího incidentu
Opatření	Snižuje míru hrozby nebo zranitelnosti
Integrita	Informace jsou správné a úplné
Důvěrnost	Informace jsou přístupné pouze oprávněným osobám
Dostupnost	Informace jsou pro oprávněné uživatele dostupné v okamžiku jejich potřeby
Bezpečnost informací	Ochrana informací před narušením důvěrnosti, integrity a dostupnosti

Riziko může být také definováno jako pravděpodobnost vzniku nežádoucího jevu konkrétního aktiva v daném čase a prostoru. Matematicky lze tento vztah popsat následující rovnicí:

$$R = P * D,$$

kde R představuje riziko,

P je pravděpodobnost, že nežádoucí jev nastane,

D jsou důsledky uskutečnění nežádoucích jevů [2].

Důsledek negativní události může mít různé podoby, jako je např. škoda na majetku, finanční újma, počet vadných nebo zničených výrobků apod. Riziko by nemělo být redukováno pouze na pravděpodobnost, protože zahrnuje jak samotnou pravděpodobnost, tak kvantitativní rozsah dané události. Finanční teorie obvykle definuje riziko jako volatilitu hodnoty portfolia okolo očekávané hodnoty v důsledku změn celé řady parametrů [2] [4].

Některé definice rizika nenaznačují kvantifikaci újmy, zatímco jiné vedou k nějakým číslům, nebo pokrývají riziko čisté i spekulativní. Hodnota rizika není veličina, ale odhad, přičemž se může jednat o odhad empirický nebo analytický [7].

1.1.1 Aktiva a jejich identifikace

Aktivem může být cokoliv, co má pro organizaci nějakou hodnotu, která může být působením hrozby snížena. Aktiva lze, stejně jako v účetnictví, dělit na hmotná a nehmotná. V procesu řízení rizik by měl být zhotoven seznam všech aktiv, jejich vlastníků a ohodnocení těchto aktiv. Ze seznamu by mělo být patrné, jaká aktiva jsou nejcennější. Určení vlastníků aktiv může být někdy velmi obtížné, zvláště pak určení vlastníka dat, která jsou často v analýze rizik nejcennější aktivem. Vlastníkem tohoto aktiva by měl být obecně ten, kdo data vytváří, je zodpovědný za jejich správnost, spolehlivost, provádí jejich klasifikaci a rozhoduje o tom, kdo bude mít k datům přístup [1].

1.1.2 Hrozby a jejich identifikace

Hrozbu lze definovat jako náhodnou, nebo úmyslně vyvolanou událost, která může mít negativní dopad na důvěrnost, integritu a dostupnost aktiv. Hrozby můžou pocházet z vnitřního nebo z vnějšího prostředí organizace. Její působení na aktiva může být dočasné, nebo trvalé a může se v průběhu času měnit. Dle původu lze rozdělit hrozby na enviromentální, hrozby úmyslné a neúmyslné. Jedna hrozba může vždy působit na více aktiv, a naopak jedno aktivum může být vystaveno současnému působení více hrozeb. U hrozeb způsobených lidmi lze dále rozlišovat, odkud útočník pochází, zda se jedná o cizí osobu nebo o vlastního zaměstnance či pracovníka servisní organizace. V tomto případě je nutné stanovit, jaké má útočník práva v systému a jaká je pravděpodobnost, že dojde k jeho odhalení a dopadení.

Opět by měl být zhotoven seznam hrozeb včetně jejich původu a toho, na jaká aktiva a na jaké atributy bezpečnosti hrozba působí. Součástí seznamu hrozeb by mělo být také ohodnocení hrozeb, ze kterého bude zřejmé, které hrozby společnost nejvíce ohrožují [1].

1.1.3 Zranitelnosti a jejich identifikace

Zranitelnost představuje slabé místo aktiva, které může být zneužito hrozbou. Míra zranitelnosti určuje, jak je aktivum vůči působení hrozby odolné, nebo jak se může hrozba projevit. Při identifikaci zranitelností se stanovují slabá místa na úrovni fyzické, logické, organizační, personální a technické bezpečnosti, která by mohla být zneužita hrozbou. Míra zranitelnosti je totiž dána úrovní stávajících bezpečnostních opatření.

Při identifikování zranitelností by měl být zhotoven seznam zranitelností, kde budou uvedena všechna opatření s popisem, jaká aktiva a před jakými hrozbami aktiva chrání. Poté se stanoví míra zranitelnosti pro každou hrozbu a aktivum. Ze seznamu by mělo být jasné, které zranitelnosti jsou největší [1].

1.1.4 Členění rizik

Z hlediska komplexního přístupu k rizikům je nutné mít přehled o různých typech rizik. Podstata komplexního přístupu k rizikům spočívá v průniku hodnocení daného rizika podle různých aplikovatelných oblastí rizik, konkrétně oblastí technických, přírodovědných, humanitních, ekonomických a případně i politických. V následující části je uvedeno členění rizik podle různých kategorií [2].

Kritérium „obor analýzy rizik“

- oblast vyšší moci,
- oblast pracovních činností,
- oblast techniky,
- oblast ekonomiky a podnikání,
- rizika v podnikání bank,
- oblast informačních rizik,
- oblast zdravotních rizik,
- projektová rizika,
- oblast ekologických rizik,
- bezpečnostní rizika,
- logistická rizika a další [2].

Kritérium ztráty a přínosu rizika

Jak bylo již uvedeno výše, riziko je vymezeno jako pravděpodobnost vzniku nestandardního jevu u konkrétního aktiva. Záporným odchylkám odpovídají negativní důsledky rizika a kladným odchylkám pozitivní důsledky. Negativní důsledky rizika jsou spojována s pojmem čistá rizika a pozitivní důsledky s pojmem spekulativní rizika [2].

Kritérium míry ovlivnitelnosti rizik

Ovlivnitelná rizika jsou taková, která můžou být ovlivňována ve prospěch subjektu. Např. zvýšením kvality výrobků a kvality servisu lze ovlivňovat objem prodeje a jejich cenu. Oproti tomu neovlivnitelná rizika jsou taková, u nichž neexistuje možnost působit na příčiny jejich vzniku, ale mohou být přijata opatření snižující nepříznivé důsledky těchto rizik. Jedná se např. o rizika politická, hospodářská apod. [2].

Kritérium systematizace rizika

Systematické riziko, je-li ekonomické, je vzhledem ke svému charakteru makroekonomické. To znamená, že je vyvoláno společnými faktory a mění se v závislosti na celkovém ekonomickém vývoji. V různé míře postihuje všechny hospodářské jednotky.

Nesystematické riziko je jedinečné a není závislé na celkovém ekonomickém vývoji. Je specifické pro konkrétní společnost, případně jejich aktivity. Tato rizika, vzhledem ke svému charakteru, představují rizika mikroekonomická [2].

1.2 RIZIKOVÉ INŽENÝRSTVÍ

Rizikové inženýrství a řízení rizik jsou dvě úzce provázané disciplíny, které se doplňují. Mají mnoho společného, přesto se liší v náplni a v cílech. Tyto obory je někdy obtížné rozlišit, nebo nadřadit jeden druhému. Bez rizikového inženýrství by nebylo možné rizika analyzovat a bez řízení rizik by práce rizikových inženýrů postrádala smysl. Řízení rizik přejímá od rizikového inženýrství výsledky, a rizikové inženýrství získává od řízení rizik podněty a požadavky [7].

Rizikové inženýrství dosud není vykládáno jednoznačným způsobem. Vždy záleží na tom, v jakém oboru je rizikové inženýrství uplatňováno. Například v pojišťovnictví rizikové inženýrství umožňuje postihnout úroveň nebezpečí a napomáhá také rizikům předcházet. Jedná se o systematické využití inženýrských znalostí a zkušeností pro optimalizaci ochrany

lidských životů, životního prostředí, majetku a ekonomických zájmů. Hlavním cílem je snížení všech typů škod a ztrát.

Z metodického hlediska se dá rizikové inženýrství chápat jako proces hledající všechny potenciální stavy, jež by ohrožovaly úspěšné fungování systému ve všech etapách jeho životnosti. Metodologie rizikového inženýrství využívá integrovaným způsobem kvalitativní a kvantitativní přístupy k riziku a systémové bezpečnosti a k rizikovému inženýrství. Základní principy kvalifikované analýzy rizik jsou následující.

Analýza rizik by měla být stavena na přístupech vědeckého myšlení, nikoliv pouze na vyplňování tabulek. Tato analýza plánovitě počítá s nejistotou a neurčitostí v procesech, které probíhají ve sledovaném systému a jeho okolí, a integruje analytické nástroje z různých disciplín. Cílem analýzy rizik je určit odezvu na různé okolnosti. V rizikovém inženýrství musí být uplatňován víceoborový přístup, tzn., že musí být použity speciální techniky a tým expertů z různých oborů [3].

Cílem rizikového inženýrství je tedy dodávat poklady o rozhodování o riziku a cílem řízení rizik je ovládat riziko a rozhodovat o riziku. Řízení rizik také tvoří cesty a postupy, které vedou k omezení nebo vyloučení dopadů nežádoucích situací a využívá nejistot ve prospěch zvýšení hodnot spekulací [7].

1.3 SPOLEHLIVOSTNÍ INŽENÝRSTVÍ

Spolehlivost je schopnost objektu nebo procesu plnit předpokládanou funkci v předpokládaném prostoru po celou předpokládanou dobu. Spolehlivostní inženýrství podporuje samotné řízení rizik. Význam pojmu spolehlivostní inženýrství lze snadno pochopit z popisu kvalifikace a náplni práce spolehlivostního inženýra. Jedná se o odborníka, který:

- ovládá principy hodnocení vlastností objektů a procesů,
- ovládá analýzu způsobů poruch a jejich následků,
- je schopen plánovat, realizovat a vyhodnocovat zkoušky spolehlivosti,
- vyšetřuje poruchy objektů a procesů,
- pracuje se spolehlivostními softwary, formuluje programy řízení spolehlivosti pro celý životní cyklus procesu,
- navrhuje zlepšení spolehlivosti, udržovatelnosti, bezpečnosti a jiných vlastností systému,

- vyjadřuje se k dokumentaci projektů a jiným podkladům.

Jádrem spolehlivostního inženýrství je ucelený soubor teoretických a empirických poznatků, uspořádaných do matematického, statistického a pravděpodobnostního rámce znalostí, matematických modelů a systémového myšlení. Znalost základních metod a postupů teorie spolehlivosti je podmínkou porozumění teorii rizika [7].

1.4 ŘÍZENÍ RIZIK

Řízení rizik je proces, při němž se snaží řídící subjekt zamezit působení již existujícím, nebo budoucím hrozbám a navrhuje řešení, která pomáhají snižovat dopad nežádoucích vlivů. Součást tohoto procesu je rozhodovací proces, který vychází z analýzy rizika. Po zvážení zejména ekonomických a technických faktorů, risk management vyvíjí, analyzuje a srovnává preventivní a regulační opatření.

Výběr optimálního řešení je kritickou fází procesu řízení rizik. Zahrnuje určení úrovně rizika, hodnocení ekonomických nákladů variantních řešení a jejich ekonomických přínosů. Zhodnocuje důsledky přijatého rozhodnutí na subjekt a jeho okolí. Následuje rozhodnutí o realizaci opatření a jeho dalším sledování.

Finálním výsledkem každé etapy řízení rizik, je rozhodnutí. Nepřijatelná úroveň rizika vyžaduje zastavení probíhajícího procesu a přijetí opatření na snížení rizika. Pro rizika, která nelze opatřením snížit, jsou vytvářeny krizové plány. Je nutné klást velký důraz na fázi redukce rizika tak, aby krizové plány byly zpracovány jen na zbytková rizika, která nelze snížit opatřením. Hledáním obecně platných preventivních opatření pro snížení pravděpodobnosti vzniku krizí a omezení jejich případných následků se zabývá také nouzové plánování, které je základní součástí krizového řízení.

Řízení rizik využívá principu zpětné nebo predikační vazby. Protože je často nereálné mít k dispozici komplexní informace a předem odhadnout vliv a význam jednotlivých faktorů, které na subjekt působí, existuje zde možnost rozhodování se za neúplné informace (fuzzy), což lze do jisté míry eliminovat pomocí nástrojů pro podporu rozhodování při neúplných informacích.

Základní oblasti, kde je uplatňováno řízení rizik, jsou následující:

- přírodní katastrofy a havárie (technologická rizika),
- rizika ochrany životního prostředí,

- finanční rizika (investiční, pojišťovací),
- projektová rizika,
- obchodní rizika (marketingové, strategické, rozpočtové, riziko managementu),
- technická rizika (inženýrské konstrukce včetně materiálů a staveb) [4].

1.4.1 Základní principy řízení rizik

Řízení rizik je metodologická disciplína, která se začala intenzivně rozvíjet po roce 1990. V současné době se metodiky soustřeďují zejména na management rizik v podnicích a organizacích, respektive projekt management. Norma ČSN ISO 31000:2009 stanovuje následující základní principy managementu rizik.

- vytváření a chránění hodnot – management rizik pomáhá k dosažení cílů a zlepšování výkonnosti v oblasti zabezpečení, ochrany životního prostředí, kvality produktů, projekt managementu, efektivnosti a v dalších oblastech,
- integrální část všech procesů v organizaci – management rizik je součástí odpovědnostního managementu a součástí všech činností v organizaci, včetně strategického plánování, projektování a implementace změn,
- součást rozhodování – management rizik se zaměřuje na nejistoty a jejich povahu,
- systematický a strukturovaný přístup – tento přístup vede k účinným, měřitelným a spolehlivým výsledkům
- dostupné zdroje informací – management rizik vychází ze zdrojů informací jako jsou údaje z minulého sledovaného období, predikce, expertní posouzení apod.,
- transparentnost a komplexnost – management rizik je adekvátní a aktuální, pokud jsou zapojeni ti, kteří odpovídají za rozhodování na všech úrovních organizace. Toto zapojení přispívá k řádnému zastoupení a zohlednění názorů těchto zainteresovaných stran při určování kritérií rizik,
- reakce na změny – management rizik neustále vnímá změny a reaguje na ně, provádí monitoring a přezkoumává nová rizika,
- neustálé zlepšování organizace [9].

1.4.2 Cíle řízení rizik

Cílem řízení rizik je rizika identifikovat a vyhodnotit, což zahrnuje zjištění možné velikosti ztráty, zjištění pravděpodobnosti výskytu a také uspořádání priorit. Rizikům, u nichž je dopad nejvyšší, je třeba věnovat vyšší pozornost ve srovnání s ostatními riziky.

Rizika je vhodnější seřadit podle obecné klasifikace do skupin kritické, důležité a běžné, namísto číselného seřazení podle dopadu. Jakékoliv ohrožení, které by představovalo katastrofu, se řadí do stejné kategorie. Je například jen malý rozdíl, když k bankrotu podniku dojde vinou ztrát z neuhrazených závazků, vinou přírodní katastrofy, nebo vinou špatného řízení podniku. Čistý efekt je stejný [4].

Cíle v oblasti řízení rizik musí být konzistentní s těmi, které si management vytyčil v oblasti strategického řízení podniku. Jestliže je strategickým cílem přežití, pak musí být pozornost managementu směřována na snížení nákladů v souvislosti s diverzifikací odbytu či nákupu. Cíle v oblasti snižování rizika budou soustřeďovány na výběr vhodné metody zajištění obchodních kontraktů s novými partnery a zjišťování jejich solventnosti. Pokud je ale strategií firmy kontinuální růst, pak se zaměří spíše na snížení rizika v oblasti řízení finančních zdrojů [6].

1.4.3 Metody snižování rizik

Vhodnost nástrojů řízení rizik v dané situaci určuje charakteristika samotného rizika. Uvedené nástroje by měly být použity v situaci, kdy je nejvýhodnějším a nejméně nákladným způsobem dosaženo cíle v podobě snížení rizika, nebo jeho úplné eliminace. V tabulce č. 2 jsou seřazena rizika do čtyř skupin podle pravděpodobnosti a tvrdosti každého rizika. Její využití je vhodné zejména ve fázi analýzy konkrétního rizika a rizikové politiky organizace [4].

Tabulka č. 2 - Metody snižování rizik [4]

Tvrdost / Pravděpodobnost	**Vysoká pravděpodobnost**	**Nízká pravděpodobnost**
Vysoká tvrdost	Vyhnutí se riziku, redukce	Pojištění
Nízká tvrdost	Akceptace, redukce	Akceptace, monitoring

1.4.4 Monitoring rizik

Vzhledem k tomu, že rizika mohou působit současně na jednu nebo více částí systému, může větší počet nízkých rizik vést v konečném důsledku ke stejné škodě, jako jedno kritické riziko. Závažnost rizika se také může měnit v čase, protože kdykoliv může dojít ke změně hodnoty dopadu, pravděpodobnosti či míry zranitelnosti. Z těchto důvodů je vhodné rizika soustavně monitorovat. Měla by být zavedena základní sada opatření, která poskytuje odpovídající úroveň ochrany. Tato sada by měla být implementována vždy a bez ohledu na aktuální výši rizika [1].

1.4.5 Akceptace rizik

Jedná se o nejběžnější metodu řízení rizik. Spočívá v tom, že subjekt riziko přijme a nic proti němu nedělá. I když je tato metoda naprosto legitimní, a v mnoha případech se může jednat o metodu nejvýhodnější, měla by být používána pouze v případech, kdy rizika povedou pouze k malým ztrátám, a pravděpodobnost jejich výskytu je spíše nízká. Použití této metody by mělo být odpovídajícím způsobem odůvodněno, tzn. o akceptaci rizika rozhodne konkrétní osoba, a o této akceptaci zhotoví písemný dokument, pod který se podepíše.

Vědomá akceptace rizika spočívá v tom, že riziko je rozpoznáno a přijato se ztrátami v něm obsaženými. Nevědomá akceptace vzniká, když je riziko nevědomě zadrženo, nebo když organizace o riziku netuší.

Obecně platí, že rizika, která mohou být zadržena, vedou k relativně malým ztrátám. Na druhou stranu, pokud se tato metoda stane jedinou strategií pro řízení rizik v podniku, může se toto rozhodnutí, kdy situace vyžadovala jiné řešení, stát fatální chybou, která může vést k ohrožení samotné existence podniku [1] [4].

1.4.6 Redukce rizik

Metoda redukce rizika je druhou nejběžnější používanou metodou. Spočívá v tom, že jsou navrhována taková opatření, která vedou ke snížení hrozeb nebo zranitelností, a tedy odstraňují samotnou příčinu rizika. Tato metoda by měla být použita v těch případech, kde se vyskytují taková rizika, jejichž frekvence výskytu je vysoká, bez ohledu na to, zda způsobují malou nebo velkou ztrátu [1].

Metoda redukce rizika je rozlišována na metody odstraňující příčinu vzniku rizika a metody snižující nepříznivé důsledky rizika.

Do první skupiny patří metody, jejichž cílem je eliminace výskytu rizikových situací. To je například přesun rizika a vertikální integrace [4].

Získávání dodatečných informací

Společnosti snižují obchodní riziko tím, že získávají dodatečné informace o svých obchodních partnerech, snaží si obstarat informace o konkurenci a o jejich dalších záměrech, provádí marketingové průzkumy a další. Snaha o získání dodatečných informací může vést ke zpoždění podnikatelských záměrů, což může firmě přinést negativní důsledky. Konkrétním příkladem tohoto způsobu snižování rizika může být chování řady českých makléřských firem, které získávají informace z jiných firem a ty využívají ve svůj prospěch [5].

Transfer rizika na jiné podnikatelské subjekty

Pro tuto metodu je charakteristický defenzivní přístup k riziku. Mezi nejčastější způsoby přesunu rizika patří:

- uzavírání dlouhodobých kupních smluv na dodávky za předem stanovené pevné ceny,
- uzavírání obchodních smluv podmiňujících odběr minimálního množství produktů,
- termínované obchody,
- odkup pohledávek,
- akreditiv, inkaso, bankovní záruka apod.,

Do druhé skupiny patří metody orientované na snížení nepříznivých důsledků. Jedná se o diverzifikaci a pojištění [4].

Diverzifikace rizika

Diverzifikace je nejčastěji využívanou metodu v investování. Hlavní myšlenou je rozložit riziko na co největší základnu. S tím souvisí i volba právní formy podnikání a to proto, aby důsledky rizika byly omezeny na předem vymezenou část soukromého majetku podnikatele. Výrobní podniky často využívají rozšíření výrobního programu. V případě poklesu poptávky po jednom produktu budou důsledky kompenzovány zvýšenou poptávkou po jiném produktu, který podnik vyrábí. V automobilovém průmyslu je často využívána geografická diverzifikace, kdy automobilové společnosti umisťují výrobní závody do zemí, kde je levná pracovní síla. Diverzifikace ale nepřináší jen užitek, ale i náklady, a zároveň je i zdrojem nových rizik. Obecně lze říci, že pravděpodobnost úspěšné aplikace této metody

v praxi je u kapitálově silné firmy mnohem větší než u firmy kapitálově slabé. Nepřipravené a unáhlené použití této metody je zejména u malých a středních firem jedním z rozhodujících kroků na cestě k bankrotu [5].

1.4.7 Pojištění

Tato metoda je vhodná pro řízení rizik, avšak ne pro zvládání rizik. I přes to, že organizace pojištění sjedná, riziko nesníží. Sníží pouze následky tohoto rizika, ale riziko přetrvává nadále. Princip pojištění spočívá ve směně velké ztráty za jistotu malé ztráty ve formě pojistného. Negativní důsledky budoucí nepříznivé situace se přenesou na pojišťovnu, která škody kryje zcela, nebo částečně. Tato metoda má smysl v případech, kdy je pravděpodobnost výskytu rizika spíše nízká, ale dopad pro společnost by byl kritický [1].

Zatímco v oblasti pojištění fyzických osob převažuje pojištění proti ztrátám na zdraví, životě a výdělku, a paradoxně majetkové pojištění je podceňováno (vyjma povinného ručení), u společností je tomu naopak. Převažuje majetkové pojištění a pojištění proti nepříznivým událostem [27].

Výhoda pojištění spočívá ve snížení objemu vázaného kapitálu, který lze výhodněji investovat. Nevýhoda spočívá v podobě nutné úhrady pojištění, ale především ve výlukách v pojištění tak, aby v případě skutečně velkých dopadů bylo možné výši pojistného plnění omezit, nebo ji zcela vyloučit [4].

1.4.8 Vyhýbání se rizikům

Tuto metodu nelze v praxi obecně doporučit, protože by to často znamenalo danou podnikatelskou činnost nedělat vůbec. Podnikatelské aktivity jsou totiž vždy spjaty s rizikem. Jedná se o negativní přístup, a pokud by byl aktivně používán, podnik by přišel o řadu příležitostí k výdělku, a s největší pravděpodobností by management nedosáhl svého cíle. Tento přístup je vhodný spíše pro nepropracované projekty, u nichž je riziko neúspěchu neúměrně velké a ztráta by byla vysoká. Dlouhodobé vyhýbání se riziku nemůže zajistit růst podniku. Existují však případy, kdy je použití této metody zcela na místě. Může se jednat například o upgrade na novou verzi operačního sytému nebo aplikace krátce po jejím uvolnění. V prvním roce uvolnění nového operačního systému se objevuje největší chybovost, proto se většinou vyplatí počkat a operační systém zavést třeba rok po uvolnění [1] [4].

1.4.9 Šíření informací o riziku

Další, velmi významnou metodou snižování rizik, je šíření informací o riziku a jeho vnímání. Tento krok je základním předpokladem k tomu, aby rizika mohla být úspěšně řízena a zvládána. Nezbytné minimum, které by měl každý manažer pro úspěšné řízení rizik udělat, je informovat management společnosti např. formou prezentace, ve které uvede zjištěná rizika a srozumitelně je vysvětlit. Poté by mělo být rozhodnuto o tom, jakým způsobem budou jednotlivá rizika zvládána a kdo bude za jejich zvládání zodpovědný. Plán by měl sestavit manažer řízení rizik spolu s top managementem společnosti. V tomto plánu by se už nemělo diskutovat o vhodnosti a volbě jednotlivých opatření, ale čistě o způsobu zvládání rizik. Tento plán by měl být následně zapracován do strategických, taktických a operativních plánů společnosti [1].

1.5 STRUKTURA ŘÍZENÍ RIZIK

Strukturovaný přístup používá norma ČSN ISO 31000:2009. Rozděluje problematiku rizik na následující fáze [9].

1.5.1 Identifikace rizik

Cílem této fáze je odhalení všech možných rizik, která budou následně řízena. Tato fáze může být rozdělena na tři etapy:

- příprava vstupních dat do procesu identifikace
- výběr vhodných metod pro identifikaci rizik
- vytvoření seznamu rizik, jejich popis a prvotní návrhy na jejich ošetření [2].

Při poslední etapě, tedy vytvoření seznamu rizik, může být využita mapa rizik. Tato mapa v grafické podobě zobrazuje priority z hlediska nakládání s rizikem. I velmi jednoduchá tabulka s identifikovanými riziky umožňuje dosáhnout vyšší efektivnosti práce s riziky. Mapa rizik může mít grafickou podobu [14].

1.5.2 Analýza rizik

Analýza rizik přináší odpověď na otázku, jak moc jsou podniková aktiva zranitelná vůči hrozbám, jak vysoká je pravděpodobnost, že hrozba zneužije určitou slabinu aktiva, a jaký by byl dopad na celý projekt nebo podnik. Je nutné brát v potaz, že hrozba může být zdrojem jednoho či více rizik a že hrozba sama o sobě riziko nepředstavuje. Hrozby pouze

zneužívají slabin vedoucí k ohrožení, což je riziko, které lze eliminovat prostřednictvím opatření chránící aktiva před působením těchto hrozeb. [12].

Stanovení hranice analýzy rizik

Hranice analýzy rizik stanovuje, která aktiva budou zahrnuta do analýzy, a která ne. Při stanovení hranice se vychází ze záměrů managementu. Aktiva, která mají vztah k cílům managementu, budou zahrnuta do analýzy a budou ležet uvnitř hranice analýzy. Ostatní aktiva budou ležet mimo hranici analýzy rizik. Aktiva, která leží uvnitř hranice, jsou ta, ze kterých je subjekt složen, nebo jsou z hlediska záměru relevantní [6].

Identifikace aktiv

Kritická aktiva jsou posuzována podle možné škody, která by vznikla omezenou funkčností nebo ztrátou aktiva. Tím se zároveň určuje i jejich hodnota. Je důležité rozlišit, zda se jedná o nenahraditelné aktivum, nebo snáze nahraditelné. Obvykle se stanovení hodnoty provádí nákladovou metodou, tedy pořizovací cenou, nebo reprodukční cenou. V případě, že aktivum přináší identifikovatelné zisky či jiné významné přínosy, může být použita i výnosová metoda. Mezi výnosové charakteristiky patří i know how, postavení na trhu, ochranná známka apod. Vzhledem k tomu, že aktiv je obvykle velké množství, provádí se seskupení aktiv podle podobných vlastností. Tím dojde ke snížení jejich počtu [4] [10].

Analýza zranitelností

V tomto kroku probíhá identifikace a kvantifikace všech slabých míst na úrovni fyzické, logické a administrativní bezpečnosti [12].

Zranitelnost je nedostatek, nebo slabina analyzovaného aktiva, nebo subjektu. Tento nedostatek může být využit hrozbou pro uplatnění jejího nežádoucího vlivu. Tato vlastnost aktiva vyjadřuje citlivost aktiva na působení dané hrozby. Každá hrozba je hodnocena vůči každému aktivu a zároveň je stanovena úroveň zranitelnosti aktiva vůči této hrozbě. Při stanovení úrovně hrozby se vychází z faktorů jako je nebezpečnost, motivace a přístup. U stanovení úrovně zranitelnosti se vychází z citlivosti a kritičnosti.

Při této analýze se berou v úvahu realizovatelná protiopatření, které mohou snížit jak úroveň hrozby, tak úroveň zranitelnosti. Výsledným stavem je soubor dvojic „hrozba-aktivum“ se stanovenou úrovní hrozby a zranitelnosti [4].

Pravděpodobnost jevu

Vzhledem k tomu, že nelze s jistotou určit, zda jev, který je zkoumán, nastane, je nutné určit údaj, s jakou pravděpodobností tento jev může nastat. Při tomto procesu se určuje, zda je jev náhodný či nikoliv a zda patří do určitého intervalu pravděpodobnosti. Dále se určuje, jaké jsou jeho další pravděpodobnostní charakteristiky a zda bude zahrnut pro přezkoumání, nebo může být vyloučen [4].

Měření rizika

Při analýze rizik se často pracuje s veličinami, které nejsou měřitelné. Určení jejich velikosti mnohdy spočívá na kvalifikovaném odhadu specialisty, který tento odhad provádí pouze na základě svých zkušeností. Velikost rizika vyplývá z hodnoty aktiva, úrovně hrozby a zranitelnosti aktiva. Pokud je riziko definováno jako možnost nepříznivé odchylky od požadovaného stavu, je stupeň rizika měřen pravděpodobností této nepříznivé odchylky. Obvykle je tento odhad stanoven na stupnici 1-10.

Čím vyšší je pravděpodobnost, že dojde k nepříznivé situaci, tím vyšší je pravděpodobnost odchylky od požadovaného výsledku, a tedy i vyšší riziko [4].

1.5.3 Hodnocení rizik

Nezbytným a nejvýznamnějším krokem při řízení rizik je výpočet míry rizik a hodnocení rizik, včetně definování rizikové pozice firmy. Po identifikaci rizik v analýze je třeba riziko vyhodnotit, což zahrnuje zjištění potenciální velikosti ztráty, zjištění pravděpodobnosti výskytu ztráty a stanovení kritičnosti těchto rizik. Rizikům, s nimiž je spojena vyšší tvrdost, je zapotřebí věnovat vyšší pozornost ve srovnání s riziky dalšími. Jakékoliv nebezpečí zahrnující ztrátu, která by představovala finanční či jinou existenční katastrofu, bude zařazeno do jedné kategorie. Podle potenciálního finančního nebo jiného dopadu ztráty lze stanovit členění rizik do jednotlivých skupin:

- kritické riziko – ohrožení, jehož ztráty jsou takového řádu, že vyústí v bankrot nebo v ukončení podnikatelské činnosti. Do této skupiny lze zařadit i ohrožení zdraví, ztráta na životech a další rizika.
- důležité riziko – ohrožení, jehož ztráty nevyústí v bankrot, ale další provoz bude vyžadovat, aby firma požádala o úvěr, nebo provedla jiné významné rozhodnutí, které svým významem přesahuje běžné hospodaření. Může se jedna třeba o odprodej aktiv apod.

- běžné riziko – ohrožení, jehož ztráty mohou být pokryty stávajícími aktivy firmy, nebo běžným příjmem, aniž by došlo k nežádoucímu finančnímu tlaku [6].

1.5.4 Ošetření rizik

Tato fáze zpravidla zahrnuje čtyři etapy.

- návrh možností nebo scénářů na ošetření rizik – zahrnují preventivní akce, které mají zabránit vzniku nebezpečí nebo snížit pravděpodobnost jejich vzniku, vypracování rezervních plánů pro případ vzniku rizika, a záchranných plánů pro případ vzniku negativního jevu,
- analýza rizik po aplikaci navržených ošetření rizik – jedná se o návrat do analýzy rizik, avšak za podmínek, kdy jsou realizovaná ošetření rizik,
- příprava plánů ošetření rizik – porovnávají se výsledky z analýzy rizik po ošetření a vybere se nejlepší scénář,
- rozhodnutí o ošetření rizik [2].

1.6 METODY ANALÝZY RIZIK

Základní hledisko pro rozdělení metod analýz rizik lze použít způsob vyjádření veličin, se kterými se v těchto analýzách pracuje. Základní přístupy řešení jsou kvalitativní a kvantitativní metody vyjádření veličin analýzy rizik, nebo jejich kombinace [4].

1.6.1 Kvalitativní metody

Tyto metody se vyznačují tím, že rizika a jejich pravděpodobnost jsou vyjádřena v určitém rozsahu diskrétní škály, např. na stupnici 1 až 10, nebo slovním popisem, např. velmi nízká až velmi vysoká. Úroveň je stanovována obvykle kvalifikovaným odhadem. Tyto metody jsou rychlejší a jednodušší, ale zároveň i více subjektivní. Obvykle přináší problémy při posuzování přijatelnosti finančních nákladů nutných na eliminaci hrozby. Tím, že chybí jednoznačné vyjádření finančních nákladů, je znesnadněna kontrola efektivnosti nákladů [4].

1.6.2 Kvantitativní metody

Tyto metody jsou založeny na matematickém výpočtu rizika z frekvence výskytu hrozby a jejího dopadu. Dopad je obvykle vyjádřen v měrných jednotkách, např. Kč a formou

roční předpokládané ztráty. Na provedení těchto metod je většinou zapotřebí více času než u kvalitativních metod. Poskytují však finanční vyjádření rizik, které usnadní jejich celkové řízení. Nevýhodou těchto metod je často vysoce formalizovaný postup, který může vést k tomu, že nebudou postihnuta specifika posuzovaného subjektu. Hodnotitel je totiž zahlcen značným objemem formálně strukturovaných dat. Tím může být zvýšena zranitelnost subjektu [4].

1.6.3 Vlastní metody

Mezinárodní normy a standardy umožňují použití i vlastní metodiky pro zhotovení analýzy rizik. Požadavkem na tyto metodiky je, kromě zjištění opakovatelných a měřitelných výsledků, zvýšení závažnosti aktiva při zvýšení kterékoliv hodnoty aktiva, jako je hrozba a zranitelnost. Základním předpokladem k efektivnímu provedený analýzy rizik je co nejlépe poznat prostředí, v němž subjekt provádí podnikatelskou činnost, a porozumět procesům, které zde probíhají. Předmětem analýzy rizik jsou tedy zejména procesy, a proto jsou vlastní metody odlišné od kvantitativních metod. Tyto metody totiž zkoumají přímo aktiva, aniž by vzaly v úvahu proces, do jakého jsou zapojeny [1].

1.7 POSUZOVÁNÍ NEBEZPEČÍ POMOCÍ METOD FMEA A FMECA

V této části práce je popsána vybraná kvalitativní metoda posuzování rizik a její postup. V praktické části práce byla použita dle zadání metoda FMECA.

1.7.1 FMEA

FMEA je zkratka z anglického Failure Mode Effect Analysis, tedy analýza způsobů a důsledků poruch. Jedná se o metodu expertní kvalitativní analýzy rizik. Tato systematická metoda je prováděna za účelem zjištění potenciálních způsobů poruch, jejich příčin a důsledků na technické parametry systému. Termín systém je představitelem hardwaru, softwaru nebo procesu. Tato analýza bývá zpravidla zahájena, jakmile je systém dostatečně vymezen, aby mohl být prezentován jako funkční blokový diagram, ve kterém mohou být stanoveny technické parametry jeho prvků.

Zásadně důležité je načasování analýzy. Jestliže se provádí dostatečně brzy v cyklu vývoje, potom může být začlenění změn návrhu k překonání nedostatků zjištěných analýzou FMEA nákladově efektivní. Je tedy velmi důležité, aby byla FMEA a její očekávané výsledky začleněny do plánu a harmonogramu vývoje. Dá se tedy definovat, že FMEA je iterativní

proces, který probíhá současně s procesem návrhu. Tento proces se aktualizuje tak, jak se návrh vyvíjí. Po změnách návrhu je pravidla nutné, aby byly příslušné části analýzy FMEA přezkoumány a aktualizovány.

Analýza je použitelná na různých stupních systému od nejvyššího stupně blokového diagramu k funkcím jednotlivých součástí nebo softwarových příkazů. Je výsledkem práce týmu složeného z jednotlivců způsobilých rozpoznat a posoudit velikost a následky různých druhů potenciálních nedostatků návrhu produktu, které by mohly vést k poruchám. Výhodou této týmové práce je zajištění nezbytné odborné kvalifikace.

FMEA je považována za metodu zjišťování závažnosti potenciálních způsobů poruch a poskytování vstupu pro opatření k jejich zmírnění, aby došlo ke snížení rizika. V některých aplikacích se však do analýzy zahrnuje i odhad pravděpodobnosti výskytu způsobů poruch. Poskytnutím určité míry pravděpodobnosti výskytu se analýza zdokonaluje.

Použití analýzy předchází hierarchické rozčlenění systému na základnější prvky. Ke znázornění tohoto rozčlenění je užitečné použít jednoduché blokové diagramy. Při analýze se postupuje způsobem zdola nahoru, tedy od prvků na nejnižším stupni po prvky na nejvyšším stupni [8].

Cíle analýzy FMEA

Cíle analýzy FMEA jsou:

- zjištění poruch, které mají nežádoucí důsledky pro provoz systému, např. znemožňují nebo významně zhoršují provoz, nebo ovlivňují bezpečnost uživatele,
- splnění požadavků smlouvy se zákazníkem, pokud jsou v ní uvedeny,
- možnost zlepšení bezporuchovosti nebo bezpečnosti systému, např. modifikacemi návrhu nebo opatřením k zajištění kvality.
- možnosti zlepšení udržovatelnosti systému, např. zvýrazněním oblasti rizika nebo neshody týkající se udržovatelnosti [8].

Provedení analýzy FMEA

Způsob provádění a prezentace analýzy může být rozdílný. Analýza je obvykle prováděna zjištěním způsobů poruch, jejich příčin a bezprostředních a konečných důsledků. Výsledky analýzy jsou zpravidla prezentovány v pracovních listech, které obsahují jádro zásadně

důležitých informací pro celý systém. Postup analýzy FMEA se skládá z následujících čtyř hlavních etap:

- stanovení základních pravidel provádění analýzy, plánování a vypracování harmonogramu, aby bylo zajištěno, že je k provedení analýzy k dispozici dostatečná doba a odborná kvalifikace,
- provedení analýzy s použitím vhodného pracovního listu či jiných prostředků, jako jsou logické diagramy nebo stromy poruchových stavů,
- shrnutí a vypracování zprávy o analýze, která bude obsahovat závěry a příslušná doporučení,
- aktualizace analýzy, jakmile pokročí vývojové činnosti [8].

Analýza FMEA je rozlišována na systémovou FMEA, konstrukční FMEA a procesní FMEA. Hlavními přínosy procesní analýzy jsou:

- zabránění nákladným modifikacím díky včasnému zjištění nedostatků návrhu,
- zjištění poruch, které mají nepřijatelné nebo významné důsledky a stanovení způsobu poruch, které mohou významně ovlivňovat očekávaný či požadovaný provoz,
- stanovení potřebnosti návrhových metod používaných pro zlepšení bezporuchovosti (zálohování, bezpečnost při poruše, volba součástí a odlehčení a další),
- sestavení logického modelu nutného k vyhodnocení pravděpodobnosti nebo intenzity výskytu abnormálních provozních podmínek systému,
- odhalení oblasti s problémy, které se vztahují k bezpečnosti nebo odpovědnosti za škody způsobené produktem, nebo zjištění neshody s požadavky nařízení a předpisů,
- soustředění se na klíčové oblasti jako je řízení kvality, kontrola a řízení procesu výroby,
- umožnění návrhářům pochopení faktorů, které ovlivňují bezporuchovost systému,

- vypracování konečného dokumentu, které je faktickým důkazem, že návrh bude v provozu splňovat svou specifikaci.

Nevýhodou této analýzy je obtížnost a zdlouhavost, zejména když je použita v případě složitých systémů, které mají mnoho funkcí, do nichž jsou zapojeny různé soubory součástí systému. Dalším nedostatkem je, že tato analýza nezahrnuje vztahy mezi jednotlivými skupinami poruch, jejich příčinami a následky. Vzhledem k interakcím software/hardware, kde předpoklad nezávislosti neplatí, je tento nedostatek ještě významnějším. Tato analýza také není schopna poskytnout ukazatele celkové bezporuchovosti systému [8].

1.7.2 FMECA

Analýza FMECA (Failure Mode, Effect and Criticality Analysis) je rozšířenou variantou analýzy FMEA. Písmeno C přidané do zkratky FMEA vyznačuje, že se do této analýzy zahrnuje i analýza kritičnosti. Stanovení kritičnosti znamená přidání do kvantitativního ukazatele velikost důsledku způsobu poruch. Kritičnost představuje dopad nebo významnost způsobu poruchy, která vyžaduje zaměření pozornosti a zmírnění této významnosti. Účelem analýzy kritičnosti je kvantifikovat relativní velikost každého důsledku poruchy jako prostředek pomáhající při rozhodování tak, aby mohla být pomocí kombinace závažnosti a četnosti výskytu stanovena priorita opatření vedoucí ke zmírnění nebo minimalizace důsledků poruch.

Jednou z metod kvantitativního stanovení kritičnosti je číslo priority rizika RPN (Risk Priority Number). Riziko je hodnoceno subjektivním ukazatelem závažnosti důsledku a odhadem očekávané pravděpodobnosti jeho výskytu v předem stanoveném časovém období. Obecný vztah ukazatele potenciálního rizika R v analýze FMECA se může vyjadřovat takto:

$$R = S * P$$

kde

S je bezrozměrné číslo, které klasifikuje závažnost (odhad), jak silně budou důsledky poruchy ovlivňovat systém nebo uživatele,

P je bezrozměrné číslo, které vyznačuje pravděpodobnost výskytu, tedy že nastane daný důsledek poruchy.

Číslo priority rizika může být použito ke stanovení priority při zaměřování se na zmírnění způsobů poruch. Kromě velikosti čísla priority rizika má na rozhodování o zmírňování vliv především závažnost způsobu poruch. Jestliže existují způsoby poruch s podobným nebo totožným číslem RPN, pozornost má být zaměřena na ty způsoby poruch, které mají vyšší čísla závažnosti. Způsoby poruch jsou seřazeny podle svých RPN čísel a vysokému RPN se přiřadí vysoká priorita [8].

Cíle analýzy FMECA

Cílem analýzy FMECA a jsou následující:

- identifikace a vyhodnocení všech nežádoucích důsledků ve vymezených hranicích analyzovaného systému a posloupnost událostí, které způsobil zjištěný způsob poruchy objektu z jakýchkoliv příčin,
- stanovení kritičnosti nebo priority, zaměření pozornosti na způsob poruchy s ohledem na správnou funkci či technické parametry systému a na dopad na konkrétní proces,
- klasifikace zjištěných poruch podle příslušných charakteristik včetně snadnosti jejich detekce,
- zjištění funkčních poruch systému a odhad míry závažnosti a pravděpodobnosti poruchy,
- vypracování plánu na zlepšení návrhu, který povede ke zmírnění způsobů poruch,
- podpora vývoje efektivního plánu údržby vedoucí ke zmírnění následků nebo pravděpodobnosti vzniku poruch [8].

Nejčastější chyby ve FMEA a FMECA

Na úspěšné provedení analýzy FMEA a FMECA má vliv více faktorů. Při implementaci jakékoliv metody existují různé způsoby, jak metodu aplikovat. V následující části jsou zmíněny nejčastěji prováděné chyby, které snižují účinnost této analýzy, a kterým by se mělo předcházet.

1. FMEA je zhotovená tak, že neřeší všechny poruchové stavy. Analýza může být buď velmi obecná, nebo velmi detailní. Je nutné se ujistit, že analýza zahrnuje veškerá

rizika spojená s novou technologií i stávající technologií, která je používána v novém prostředí a všechny ostatní oblasti, které mohou být kritické,

2. Další chybou je neuvažování o rozhraní nebo o druhu poruchy spojené se systémem a integrací subsystému. Analytici se obvykle zabývají klíčovou funkcí, ale mohou přehlédnout důležité propojení, které může způsobit kritické selhání. Je nutné se ujistit, že toto propojení je zahrnuto ve vývojových diagramech včetně druhů poruch a jejich následků,
3. Analýza je provedena příliš pozdě. Tato chyba snižuje účinnost FMEA analýzy a oslabuje schopnost řídit procesní změny. FMEA by měla být provedena paralelně s procesem návrhu,
4. Poslední, velmi častou chybou, jsou nesprávní lidé v týmu. Je důležité umístit správné lidi s odbornými znalostmi do hlavního týmu. Je obzvláště důležité dostatečná podpora tohoto týmu managementem. Potenciální členové týmu mohou být zástupci z oblasti konstruktérství, systémového inženýrství, testování, výroby, kontroly kvality a dalších oborů. I přesto, že jedna osoba může analýzu výrazně usnadnit, měl by se na jejím zhotovením podílet celý tým [13].

2 PRAKTICKÁ ČÁST

V této části práce jsou uvedeny základní informace o společnosti Air Bank, a.s., portfolio služeb, organizační skupina a další obecné informace o bance. Na základě veřejně dostupných informací je provedena analýza vnitřního a vnějšího prostředí podniku a SWOT analýza. Na konci této části je popsán proces zavádění informačního systému v bance a zhotovena analýza FMECA.

2.1 PŘEDSTAVENÍ SPOLEČNOSTI

Společnost Air Bank, a.s., je bankovní instituce, která vznikla zápisem do Obchodního rejstříku dne 26.2.2010 a působí v České republice. Je součástí finanční skupiny PPF Financial Holding, B.V., která sídlí v Nizozemsku a působí po celém světě.

Obchodní firma: Air Bank a.s.

Právní forma: Akciová společnost

Sídlo: Evropská 2690/17, 160 00 PRAHA

Identifikační číslo: 290 45 371

Datum zápisu společnosti do OR: 26.2.2010

Výše základního kapitálu zapsaného v OR: 500 017 000 Kč

Výše splaceného základního kapitálu: 500 017 000 Kč

Druh akcií: kmenové akcie

Forma akcií: na jméno

Podoba akcií: zaknihované

Počet akcií: 500 017 000 ks

Nominální hodnota akcie: 1 000 Kč

Akcionáři Air Bank: PPF Group, N.V., 86,624 %

EMMA OMEGA LTD, 13,376%

Své služby začala nabízet široké veřejnosti 22.11.2011. Nabídku běžného a spořicího účtu později rozšířila o spotřebitelský úvěr a refinancování hypoték. V průběhu let 2012 až

2015 realizovala ve spolupráci s propojenými skupinami Home Credit projekt financování retailových pohledávek, a stala se tak 100% vlastníkem a ovládající osobou společnosti.

Předmětem podnikatelské činnosti společnosti Air Bank jsou činnosti zapsané v obchodním rejstříku. Jedná se o činnosti uvedené v §1 odst. 1, písm. a) a b) zákona o bankách:

- přijímání vkladů od veřejnosti,
- poskytování úvěrů,

Dále pak činnosti uvedené v §1 odst. 3, písm. a), c), d), g), i), k), l), m) a o) zákona o bankách, tj.:

- investování do cenných papírů na vlastní účet
- platební styk a zúčtování
- vydávání a správa platebních prostředků,
- obstarávání inkasa,
- finanční makléřství,
- poskytování bankovních informací,
- obchodování na vlastní účet nebo na účet klienta s devizovými hodnotami, které nejsou investičním nástrojem, a se zlatem,
- činnosti, které přímo souvisí s činnostmi uvedenými v bankovní licenci

Žádné činnosti nebyly Českou národní bankou omezeny, nebo vyloučeny [15].

2.1.1 Nabízené služby

V současné době banka nabízí základní bankovní služby fyzickým osobám, které chtějí využívat běžné bankovní služby zejména k osobním účelům. Služby uzpůsobené pro podnikatelské účely a transparentní účty pro neziskové organizace banka nenabízí.

Podnikatelé samozřejmě mohou využívat služby banky, ale některé dokumenty nebudou splňovat náležitosti, které jsou jimi často požadovány. V praxi to znamená, že na výpisech nebo potvrzeních nikdy nebude uvedeno IČO, nebo název společnosti. V tuto chvíli banka nabízí následující služby:

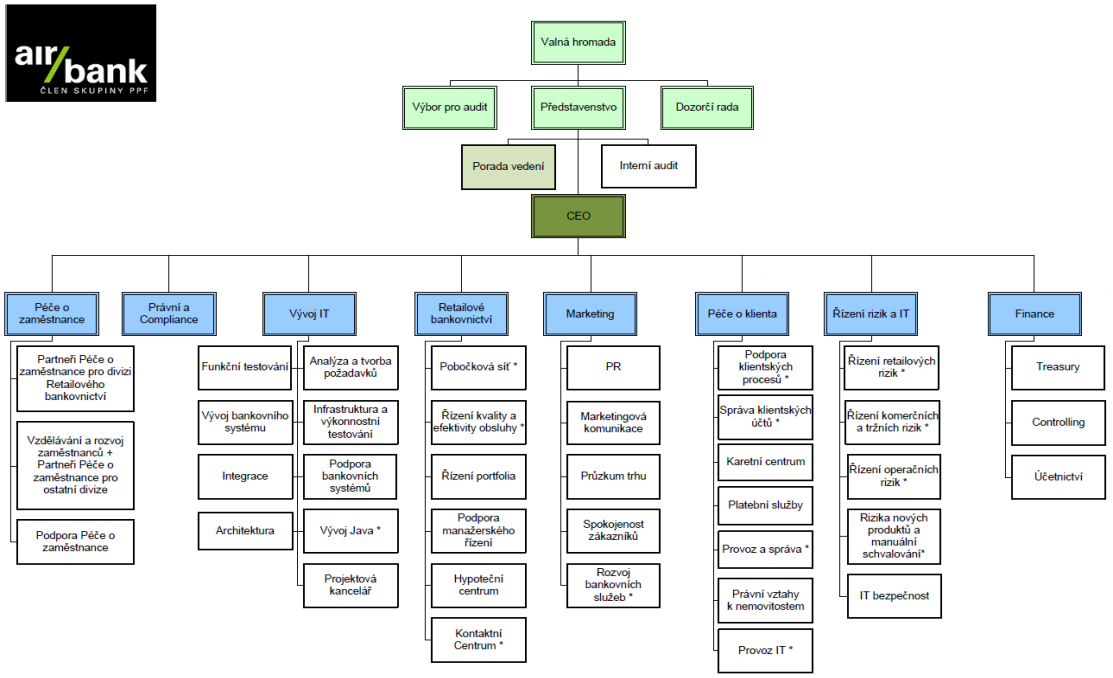
- Běžný účet

- Spořicí účet
- Pojištění pravidelných výdajů
- Pojištění pro případ invalidity a úmrtí
- Cestovní pojištění
- Spotřebitelský úvěr
- Refinancování spotřebitelského úvěru
- Refinancování hypotéky
- Převod účtu [15].

2.2 ORGANIZAČNÍ STRUKTURA

Organizační struktura společnosti vykazuje prvky liniové struktury a funkcionální. Hlavní myšlenkou funkční organizace je seskupení pracovníků, kteří pracují na podobných úkolech, v jednom úseku podniku. Funkcionální struktura je velmi běžná ve středně velkých podnicích kvůli produkci nižšího počtu výrobků nebo služeb a vysoké úrovni specializace. Tato organizační struktura centralizuje rozhodování na nejvyšší úrovni podniku. Top management je zároveň řešitelem sporů, které mohou vznikat interakcí mezi jednotlivými řediteli úseků [19] [15].

Orgány společnosti jsou valná hromada, dozorčí rada a představenstvo. Dále v podniku působí Úvěrový audit, Výbor pro řízení aktiv a pasiv, Výbor pro audit a interní audit. K 30.9.2016 je evidováno 36 obchodních a 706 pracovních míst. Obrázek č. 1 zobrazuje aktuální organizační strukturu společnosti.



Obrázek č. 1 – Organizační struktura [15]

Společnost řídí generální ředitel Michal Strcula, kterému jsou přímo podřízeni ředitel řízení rizik a IT, ředitelka péče o zaměstnance, ředitelka právního oddělení a compliance, ředitel řízení změn a spokojenosti zákazníků, ředitel marketingu, finanční ředitel, ředitelka interního auditu, ředitel vývoje IT a ředitel péče o klienta [15].

2.3 ANALÝZA VNĚJŠÍHO PROSTŘEDÍ

Pro zhotovení analýzy vnějšího prostředí bývá nejčastěji používána analýza sociálních, legislativních, ekonomických, politických a technologických faktorů (SLEPT analýza). Vzhledem k tomu, že v této práci není řešena strategie podniku, ale proces zavádění informačního systému, byl z této analýzy použit pouze faktor technologický, který významně ovlivňuje výběr a zavedení informačního systému, pro který se společnost rozhodne. V analýze tedy nebyly použity faktory politické, ekonomické, legislativní a další.

2.3.1 Technologické faktory

V současnosti, kdy je internetové bankovnictví, mobilní aplikace, bezkontaktní platby a platby prostřednictvím QR kódu součástí běžných služeb, které banky nabízí, musí banky vynakládat další náklady na vývoj a výzkum moderních technologií. Může se jednat o bezkontaktní výběr z bankomatů, platba u obchodníka prostřednictvím NFC, certifikát zabezpečení webových stránek, nové služby, aplikace, která umí číst otisk prstu nebo oční

duhovku apod. Předpokladem je, že zákazníci mají přístup k internetu buď ze svého počítače, nebo telefonu.

Informační systém musí umožnit uživateli zjistit, jak klient tyto služby využíval v minulosti i v současnosti, a případnou práci s nimi. Uživatel v informačním systému nejčastěji pracuje s:

- internetovým bankovnictvím klienta,
- jednotlivými žádostmi klienta,
- sjednanými službami,
- historií plateb,
- urgencemi a požadavky,
- reklamacemi,
- karetními transakcemi,
- písemně a telefonicky komunikuje s klientem.

Čím více má klient sjednaných služeb a čím více nových technologií klient využívá, tím může být přehlednost v informačním systému ztížena. Proto je velmi důležité, aby jednotlivé odkazy směřovali do správných integrovaných systémů a byla zaznamenávána veškerá historie přehledně podle typu kontaktu s klientem. Velmi důležité je také zaznamenávání změn stavů jednotlivých žádostí a používaných služeb, bez kterých by uživatel nemohl dohledat informace, které potřebuje dál používat.

Mobilní aplikace

Mezi nejčastěji vyhledávané služby v mobilních aplikacích patří zobrazení zůstatku a historie transakcí, stejně jako v internetového bankovnictví. Z aktivních operací se jedná o jednorázové platby, které jsou zadávány asi při každém pátém přihlášení do aplikace. Téměř všechny banky v ČR podporují systémy iOS a Android. Windows Phone už jen 9 bank, mezi něž Air Bank patří [17].

V tabulce č. 3 je zobrazen podíl klientů vybraných bank, kteří používají mobilní aplikaci.

Tabulka č. 3 - Podíl klientů vybraných bank používající mobilní aplikaci [17]

Banka	Podíl klientů v procentech
ZUNO bank	40
Air Bank	26
mBank	20
Fio Bank	10
Komerční banka	20
Raiffeisenbank	15
Equabank	25
ČSOB	23

Informační systém musí uživateli umožnit rozpoznat, které aktivní operace klient prováděl v internetovém bankovnictví a které v mobilní aplikaci. Zároveň uživatel musí mít náhled na změny stavů jednotlivých registrovaných mobilních aplikací klienta a být schopen tyto stavy měnit (blokovat, odblokovat, aktivovat a zrušit), případně pomoci aplikaci propojit s účtem klienta.

Zabezpečení internetového bankovnictví a informačního systému

Při přihlašování do internetového bankovnictví musí mít klient jistotu, že se nejedná o podvodné stránky a že web provozuje banka, u které má vedený účet. Pokud uživatel odesílá přes webové stránky osobní údaje, finanční data, nebo jiné citlivé informace, je nutné, aby komunikace mezi stránkami a návštěvníkem byla šifrovaná. Při přihlašování by si měl klient ověřit, zda se mu v adrese webové stránky zobrazuje protokol HTTPS a zda je platnost stránky ověřena certifikátem. Většina bank také nabízí klientům přihlášení pomocí SMS kódu nebo pomocí potvrzení přihlášení v mobilní aplikaci. Uživatel informačního systému, který pracuje v internetovém bankovnictví klienta, zabezpečení kontrolovat nemusí, protože přihlášení je zabezpečeno v rámci vnitřní sítě. Aktivní operace provádí s ústním souhlasem klienta. Tento ústní souhlas je uchováván v podobě nahrávky hovoru, který je archivován 10 let po ukončení smluvního vztahu.

Uživatel informačního systému se přihlásí do firemního počítače pomocí platných přihlašovacích údajů. Ti, kteří využívají firemní notebook, mají navíc data zašifrována na pevných discích. Pro ověření uživatele na síti a přidělení IP adresy musí mít uživatel platný doménový a uživatelský certifikát.

Do informačního systému se uživatel může přihlásit pouze po zadání platných přihlašovacích údajů a platných certifikátů. Uživatel má zároveň přidělena oprávnění, díky kterým může pracovat v jednotlivých částech informačního systému. Všechny úkony, které uživatel provádí, jsou zaznamenávány do textových logovacích souborů.

Přístup na server je umožněn pomocí certifikátu, který je uložen na čipové kartě správce systému. Informační systém je proti útokům zvenčí chráněn pomocí firewallu a přistupovat do vnitřní sítě může pouze určitý rozsah IP adres.

Transfer technologií

Banky, ale i jiné společnosti, mohou využívat tzv. transfer technologií. Jedná se o nalezení vhodné technologie buď ze zahraničí, nebo z České republiky, která vznikne buď v jiné společnosti, nebo výzkumné instituci. Pokud by transfer technologií byl pro Air Bank přínosem, může využít technologie, které využívají jiné společnosti v rámci skupiny První privatizační fond (dále jen PPF), nebo technologie ze zahraničí.

Výdaje na výzkum, vývoj a inovaci

Výdaje na výzkum a vývoj v roce 2015 překročily hranici 85 miliard Kč. Podíl těchto výdajů na HDP poprvé dosáhl hranici 2%, což je nadprůměrná hodnota v EU. Regionálně byl nejúspěšnějším Jihomoravský kraj, jehož podíl výdajů na HDP činil 3,5%. Jedním z důvodů tohoto nárůstu výdajů v České republice je soukromé financování výzkumu a vývoje společností působící v České republice pod zahraniční kontrolou. Společnosti investovaly do výzkumu dvakrát více finančních prostředků, než vysoké školy a třikrát více než veřejné výzkumné instituce. Nejvíce investují podniky působící v těchto odvětvích:

- automobilový průmysl,
- strojírenství
- ICT služby a programování,
- biotechnologie a nanotechnologie [21].

Air Bank v roce 2015 investovala do interně vyvinutého nehmotného majetku 67 mil Kč a do nakoupeného nehmotného majetku 165 mil Kč. Ve srovnání s rokem 2014, kdy do interně vyvinutého nehmotného majetku investovala 58 mil Kč a do nakoupeného nehmotného majetku 179 mil Kč, byly investice srovnatelné. V těchto letech dlouhodobý nehmotný majetek představoval pouze software.

2.4 ANALÝZA KONKURENČNÍHO PROSTŘEDÍ

Analýza konkurenčního prostředí, známá jako Porterova analýza, prognózuje vývoj konkurenční situace ve zkoumaném odvětví na základě odhadu možného chování zkoumaných subjektů působících na trhu. Tato analýza se zabývá následujícími subjekty:

- stávající konkurenti,
- potenciální konkurenti,
- dodavatelé,
- odběratelé
- substituti [11].

Air Bank, a.s., vstoupila na bankovní trh v roce 2011. V té době měly největší podíl na českém bankovním trhu společnosti Česká spořitelna, ČSOB a Komerční banka. Tento podíl si drží dodnes. Air Bank těmto bankám nemůže konkurovat v procentuálním podílu na trhu, nebo v objemu poskytnutých úvěrů, ale v tempu růstu. Air Bank je řízena marketingově a nejvíce investuje do budování značky a vztahu se zákazníky. Poslední ocenění, které získala, je Nejvstřícnější banka roku 2016 [18].

2.4.1 Stávající konkurence

Přímí konkurenti Air Bank jsou zejména banky, které se, stejně jako Air Bank, zaměřují na poskytování služeb fyzickým osobám, nikoliv firmám a neziskovým organizacím. V tuto chvíli takové služby nabízí pouze ZUNO a mBank. Všechny ostatní bankovní instituce poskytují služby i živnostníkům, neziskovým organizacím a korporátům.

Při úvaze o konkurenci se ale nejde zaměřit pouze na banky, které nabízí stejné služby. Je nutné brát v úvahu i další banky, které poskytují širší nabídku služeb, protože právě tyto banky jsou na trhu většinou delší dobu, mají mnohem více poboček, více klientů a dokážou často nabídnout i lepší úrok u úvěru. V tabulce č. 4 je provedeno srovnání vybraných parametrů u vybraných bank, které jsou považovány za největší konkurenty Air Bank.

Tabulka č. 4 – Srovnání bank podle vybraných ukazatelů

Ukazatel	Air Bank	Equa Bank	mBank	Česká spořitelna	ČSOB	Komerční banka	Fio banka	Raiffeisenbank
Počet klientů	460 tis	200 tis	573 tis	4,71 mil	2,9 mil	1,6 mil	670 tis	nezveřejňuje
Objem poskytnutých úvěrů	27 mil Kč	13,5 mil Kč	nezveřejňuje	548,8 mil Kč	581,7 mil Kč	548,2 mil Kč	13,3 mil Kč	189 mil Kč
Počet poboček v ČR	34	59	8	601	251	399	75	119 Kč
Poplatek za vedení základního účtu	0 Kč	0 Kč	0 Kč	0 Kč	25 Kč	68 Kč	0 Kč	99 Kč
Nejnižší možný úrok u úvěru	6,9% p.a.	5,7% p.a.	9,9% p.a.	6,9% p.a.	individuální	6,9% p.a.	8,30%	7,9% p.a.
Nejvyšší možný úrok u úvěru	9,9% p.a.	individuálně	9,9% p.a.	individuálně	individuální	individuální	18,90%	individuální
Nejnižší možný úrok u hypotéky	2,09% p.a.	1,99% p.a.	1,54% p.a.	2,19% p.a.	individuální	2,29% p.a.	1,58% p.a.	2,29% p.a.
Nejvyšší možný úrok u hypotéky	2,59% p.a.	individuálně	3,99% p.a.	individuálně	individuální	individuální	individuální	individuální
Možnost používání mobilní aplikace	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO
Hospodářský výsledek za rok 2015	309 mil Kč	ztráta 381 mil Kč	279 mil Kč	1 430 mil Kč	1 400 mil Kč	1 280 mil Kč	210 mil Kč	2 500 mil Kč

Pokud by Air Bank byla posuzována podle počtu klientů, nebo podle objemu poskytnutých úvěrů, byla by zařazena mezi menší banky. Úroková sazba, za kterou poskytuje spotřebitelské úvěry, je srovnatelná, nebo nižší, než nabízí ostatní konkurenční banky. U hypotečních úvěrů je to podobné. Úroková sazba Air Bank je srovnatelná s ostatními bankami. Otázkou tedy zůstává, jak může Air Bank obstát v konkurenčním boji o zákazníky a jaký vliv má na to informační systém, který banka používá.

Ve výsledku nemusí být rozhodující úroková sazka, ale rychlost načerpání finančních prostředků na účet. Tomu předchází kontrola dokladů a příjmů klienta. Tyto činnosti jsou prováděny manuálně, a mnohdy právě v tomto kroku dojde k největšímu zdržení procesu schválení. Informační systém musí uživateli umožnit zjistit:

- jakým způsobem klient o úvěr žádal (na pobočce, přes telefon, nebo přes internet),
- zda už nahrál požadované dokumenty do internetového bankovnictví,
- v jaké fázi ověřování se žádost nachází,
- který uživatel informačního systému žádost zpracovává,
- kdy banka pošle klientovi požadovanou částku na účet.

Přehledný informační systém může tedy urychlit celý proces žádosti o úvěr, a tím banka získává konkurenční výhodu.

Proces zakládání bankovních účtů je o něco jednodušší a rychlejší, nicméně požadavky klienta jsou rozdílné. V současné době, kdy úrokové sazby jsou velmi nízké, klienti vyhledávají takové účty, které jim aspoň trochu zhodnotí peníze, které mají u banky uložené. Pro banky je úročení těchto vkladů v současné době drahou záležitostí, a tak úročení účtů omezují různými limity, nebo podmínkami. Air Bank nabízí úročení jak spořicího, tak běžného účtu, ale pouze za předpokladu, že klient zaplatí alespoň pětkrát v měsíci platební kartou v obchodě, nebo na internetu. Za tyto karetní transakce totiž obchodník odvádí bance určité procento z platby. Tímto způsobem banka dorovnává náklady na úročení účtů klientů.

Požadavky na informační systém v rámci zakládání účtů a převádění účtů z jiných bank jsou podobné, jako u žádostí o úvěr. Informační systému musí umožnit uživatelům zjistit:

- jakým způsobem klient podal žádost o účet,
- zda klient dodal požadované doklady a jakým způsobem,
- v jaké fázi schválení se žádost nachází,
- zda klient dodatečně žádal o další doplňkové služby,
- zda již byla odeslána platební karta klientovi a na jakou adresu,
- zda se platební karta nevrátila zpět,

- zda klient platební kartu aktivoval a jakým způsobem.

Informační systém tedy může urychlit proces založení účtu, ale v tomto případě se nejedná o významnou konkurenční výhodu. Žadatelé o účet málokdy na aktivaci účtu spěchají tak, jako na vyřízení žádosti o úvěr. V tomto případě hrají větší roli poplatky za služby a úroková sazba na spořicím účtu, jejichž výše je dána spíše strategií podniku.

2.4.2 Potenciální konkurence

Potenciální konkurenti společnosti Air Bank mohou být následující:

- nebankovní instituce, které budou splňovat podmínky pro získání bankovní licence a požádají o ni,
- zahraniční banky, které mají v plánu expandovat na český trh.

Hrozba vstupu na bankovní odvětví není tak vysoká, jako např. u jiných odvětví. Všechny banky v České republice podléhají kontrole České národní banky, která jim uděluje a prodlužuje licenci. U akciových společností je zapotřebí vysoký základní kapitál. Čeští klienti jsou často skeptičtí, co se týče nových bank a většinou chtějí mít záruku, že banka nezbrankrotuje. Když Air Bank nově vstoupila v roce 2011 na trh, byla, a stále je součástí finanční skupiny PPF, do které patří například i Home Credit. Tato skutečnost mohla být jeden z důvodů, proč si banka rychle získala velký počet klientů. Významný investor v pozadí je pro mnoho zákazníků záruka, že banka během prvních let nezbrankrotuje.

Potenciální konkurenti, zejména zahraniční banky, mohou využívat lepší technologie a informační systém, který zajistí rychlejší vyřízení požadavku klienta a lepší zákaznickou podporu.

2.4.3 Dodavatelé

Hlavními dodavateli Air Bank jsou:

- MasterCard – výrobce platebních karet
- poskytovatel informačního systému,
- poskytoval internetového a telefonického připojení,
- dodavatel PC a jejich komplementů,
- jiné komerční banky, které můžou Air Bank poskytnout úvěr,

- poskytovatelé mobilních aplikací.

Vyjednávací síla dodavatelů je u každého z dodavatelů jiná. Poskytovatel internetového a telefonického připojení bude mít pravděpodobně nižší vyjednávací sílu než zhotovitel informačního systému.

Vyjednávací síla poskytovatele informačního systému je velká z důvodu omezeného počtu potenciálních zhotovitelů, kteří dokáží vyhovět požadavkům banky.

2.4.4 Odběratelé

Air Bank se zaměřuje pouze na jednu cílovou skupinu zákazníků, a to jsou fyzické osoby, které chtějí využívat bankovní služby zejména k osobním účelům. Banka se nezaměřuje na právnické osoby ani na neziskové organizace. Nabídku služeb postupně rozšiřuje podle zvolené strategie a podle výsledků z dotazníkového šetření svých klientů.

Kupní síla klientů banky je malá. Klient nemá možnost vyjednat individuální podmínky pro bankovní účet nebo úvěr. Banka má tyto podmínky stanovené v obchodních podmínkách a může je v průběhu trvání smlouvy s klientem měnit. Pokud klient s těmito podmínkami nesouhlasí, má pouze jedinou možnost, a to přejít k jiné bance.

Mnoho klientů upřednostňuje osobní schůzku s bankéřem na pobočce, kde řeší své požadavky. Pokud má banka málo poboček, musí tuto nevýhodu vyvážit rychlým zákaznickým servisem po telefonu, nebo písemnou komunikací. Informační systém může výrazně ovlivnit, jak rychle uživatel informačního systému klienta odbaví a poskytne klientovi všechny informace, které potřebuje. Zároveň by informační systém měl umožnit, aby uživatel byl schopen provádět úkony na účtu klienta stejně tak, jako by se klient dostavil na pobočku, nebo přímo pracovat v klientově internetovém bankovnictví. Jedině tak může banka konkurovat těm bankám, které mají mnohem hustší pobočkovou síť v České republice.

2.4.5 Substituti

Substituční produkty a služby pro spotřebitelský úvěr mohou být následující:

- nákup na splátky,
- leasing,
- kreditní karta,
- kontokorent,

- americká hypotéka,
- půjčka od známých,
- úvěr od nebankovních institucí.

Substituční služby zde uvedené jsou vždy něčím rozdílné od spotřebitelských úvěrů, například zajištěním, účelovostí, vyšší úrokovou sazbou apod. Mají ale také své výhody. U některých služeb nemusí klient prokazovat příjem, případně mu banka nebo nebankovní instituce poskytne úvěr, i když měl klient v minulosti exekuci nebo záznam v bankovním či nebankovním registru.

O tom, zda se žadatel rozhodne využít služeb Air Bank, nebo substitučních služeb, opět rozhoduje nejen úroková sazba, ale i rychlost poskytnutí úvěru. Stejně jako v části konkurenti je důležité, aby banka používala takový informační systém, který umožní co nejrychleji úvěr žadateli poskytnout.

2.5 ANALÝZA VNITŘNÍHO PROSTŘEDÍ

Pro analýzu vnitřního prostředí byla použita analýza 7S podle Mc Kinseyho [4].

Podle této analýzy je potřeba identifikovat 7 vnitřních, vzájemně se ovlivňujících faktorů, které musí být rovnoměrně rozvíjeny. Těmito faktory jsou:

- struktura firmy,
- strategie,
- schopnosti,
- sdílené hodnoty (firemní kultura),
- spolupracovníci,
- styl řízení,
- informační systém.

2.5.1 Strategie firmy

Strategie banky je dlouhodobě zaměřena na budování značky a vztahu se zákazníky. Cílem banky je nabídnout takový produkt, který mohou využívat všichni pro osobní potřeby. Nespecializuje se tedy na jednotlivé skupiny, jako jsou studenti, podnikatelé, starobní důchodci a další. Podmínky jsou stanoveny pro všechny stejné.

Každý podnik se snaží o dosažení určité konkurenční výhody. Většina bank v tomto ohledu dává přednost produktům na míru, nabídnutí nejlepšího úroku u úvěru, výhodám nově příchozím klientům apod. Air Bank se zaměřuje na flexibilitu služeb. Flexibilita u služeb znamená volnost ve využívání služeb, tj. bez různých limitů a podmínek, s možností výpovědi, předčasného doplacení úvěru apod. A to i u hypotečních úvěrů, u kterých je u ostatních bank velmi obtížné předčasné splacení provést. Co se týče zákaznického servisu, naprostá většina požadavků lze řešit z internetového bankovnictví, nebo po telefonu. Klienti tedy nemusí chodit na pobočku, ve většině případů nemusí dokumenty posílat poštou v originále apod. Tuto možnost ocení hlavně klienti dlouhodobě žijící v zahraničí, nebo klienti, kteří ve svém městě nemají pobočku, nebo jsou časově vytížení.

Výběr informačního systému se odvíjí od podnikové strategie a reálným budoucím potřebám firmy. Informační systém, který je nástrojem pro zpracování všech firemních informací, slouží jako základna pro všechny další aplikace a systémy. Funkčnost informačního systému a možnost informačních technologií je významnou příležitostí pro otevření nových horizontů při hledání strategických možností rozvoje firmy. Špatné rozhodnutí v oblasti volby informačního systému může omezit možnost dalšího rozvoje. Důležité je také stanovit, jaký podíl investic do informačních technologií vytváří konkurenční výhodu, která je v daném oboru nová a jakým způsobem informační technologie přispívají k růstu tržeb [20].

2.5.2 Organizační struktura

Organizační struktura Air Bank vykazuje prvky liniové a funkcionální organizační struktury. Organizační struktuře musí odpovídat i návrh informačního systému. Někdy společnosti používají více informačních systémů najednou, protože jeden implementovaný informační systém nemusí komplexně vyhovět potřebám organizace. Více informačních systémů dokáží plnit všechny úlohy pro jeden společný nadřazený systém, který slouží zejména ke sběru, zpracování a předání potřebných informací. Tyto informační systémy je možné používat odděleně a integraci provádět manuálně. Nabízí se i možnost systémové integrace, která může být náročná, ale přináší mnoho výhod.

Při volbě informačního systému vhodného pro danou organizaci je zapotřebí také zvolit, zda organizace dá přednost univerzálnímu informačnímu systému, který využívají i jiné podniky, nebo zvolí zhotovení informačního systému na míru.

2.5.3 Informační systémy

Informační systém, který banka používá, je jednotný. V závislosti na náplni práce používají uživatelé další programy a aplikace, s nimiž pracují. Informační systém má zejména usnadňovat a zrychlovat práci zaměstnanců. Pokud je ale informační systém příliš komplikovaný, může práci uživatelů naopak zpomalit. Cílem je vytvořit pracovní místo, ze kterého bude mít uživatel přístup do všech programů a aplikací, které k práci potřebuje. Zároveň banka používá takový informační systém, ze kterého může vytvářet kvalifikované reporty pro sledování výkonnosti zaměstnanců.

2.5.4 Styl řízení

V Air Bank je styl řízení demokratický. Vedení jednotlivých oddělení dává možnost pracovníkům vyjádřit se, případně jim umožňuje podílet se na zlepšování procesů jak v oddělení, ve kterém pracují, tak i v jiných odděleních, která jsou spolu úzce propojena. Část svých pravomocí vedoucí pracovníci delegují na podřízené pracovníky a část pravomocí si ponechávají. Zároveň rozhodují v konečných rozhodnutích. Komunikace uvnitř banky je tedy obousměrná. Výhodou tohoto typu řízení je účast podřízených pracovníků na rozhodování a pocit sounáležitosti, což přispívá k upevnění firemní kultury. Nevýhodou je určitá časová ztráta spojená s demokratickým řízením, která je ale často vynahrazena zlepšováním procesů a efektivitou [4].

Souvislost mezi stylem řízení a informačním systémem spočívá v tom, jak moc jsou uživatelé informačního systému kontrolováni nejen z pohledu úkonů, ale zejména z pohledu efektivity práce. Informační systém může poskytnout report, kolik času uživatel strávil řešením jednotlivých úkolů, jak úkoly splnil nebo ještě nesplnil, a může pomoci při dohledání u rozpracovaných úkolů, kdo přesně se na splnění tohoto úkolu podílel.

2.5.5 Spolupracovníci

Lidé jsou jedním z hlavních zdrojů každého podniku, který může vést ke zvyšování výkonnosti, ale také k úpadku. V bankovním sektoru je velmi důležitá pověst v očích veřejnosti, kterou můžou výrazně poškodit pracovníci banky, kteří jsou v přímém kontaktu s klienty. Další úskalí spočívá v podvodném jednání zaměstnanců. Toto riziko může banka snížit správným výběrem pracovníků, kteří svým charakterem zapadají do firemní kultury a zároveň mají předpoklady k vybrané pozici. Dále banka zavádí taková kontrolní opatření,

díky kterým se zaměstnanec banky nemůže dopustit podvodného jednání. Jedná se zejména o monitorování činností zaměstnance, přístupová práva k informacím a průběžnou kontrolu [4].

Air Bank, která se snaží v první řadě o budování dobrých vztahů s klienty. Proto udržuje přátelskou firemní kulturu, kde má každý pracovník možnost vyjádřit se k procesům v bance, k motivačnímu systému, k produktovým novinkám a dalším věcem. Větší efektivitu zaměstnanců nepodněcuje pomocí příkazů, ale pomocí různých soutěží, za které můžou zaměstnanci získat zajímavé odměny a ceny. Všechny tyto zdánlivé drobnosti ovlivňují přístup zaměstnanců ke klientům, protože přátelské pracovní prostředí se výrazně odráží na náladě a celkové výkonnosti pracovníků.

2.5.6 Sdílené hodnoty

Sdílené hodnoty představují určité vzorce chování na pracovišti, etický kodex a vnitřní atmosféru firmy. Velmi úzce souvisí s částí spolupracovníci, protože právě pracovníci banky se podílejí na vytváření a udržení sdílených hodnot. V Air Bank je zavedeno desatero sdílených hodnot jak pro vztah pracovníků banky s klientem, tak pro vztahy mezi pracovníky. Důležité je, aby komunikace s klientem byla vždy srozumitelná. Air Bank je česká banka, a proto je internetové bankovnictví a všechny smlouvy s klientem vedeny pouze v českém jazyce. Pracovníci banky se také vyhýbají velmi odborným výrazům při komunikaci s klientem, aby se vyhnuli možným nedorozuměním.

2.5.7 Schopnosti

Při stanovení požadavků na schopnosti a dovednosti pracovníků je potřeba rozlišovat, o jakou pracovní pozici se jedná a zda jsou vítané zkušenosti, které pracovník získal v předchozím zaměstnání. V mnoha případech je totiž lepší pracovníka učit novým věcem než ho přeučovat. Při provádění činností, které má pracovník už zautomatizované a je si v nich velmi jistý, dochází k nejvíce pochybením. Mezi nejvíce oceňované schopnosti v Air Bank patří schopnost učit se novým věcem a hledat nová řešení. Jeden z faktorů úspěchu je schopnost rychle se adaptovat na změny, a pokud by pracovníci banky pracovali jen podle zažitých postupů a neposuzovali některé záležitosti individuálně, banka by tímto mohla přijít o spoustu klientů. Naprostá většina klientů totiž žádá individuální přístup, což je většinou nemožné provést technicky, natož časově. Přesto je nutné hledat nová řešení problémů. Na tyto nové způsoby většinou přijdou právě noví zaměstnanci banky, nebo klienti.

Mezi dovednosti, které banka po svých zaměstnancích požaduje, je schopnost pracovat v informačním systému a programech, které jsou pro konkrétní pozici nezbytné. Stejně tak důležitá je detailní znalost internetového bankovnictví a mobilní aplikace Air Bank. Uživatelé informačního systému jsou pravidelně proškolování. Aktuality a novinky jsou popsané v dokumentaci, ke které mají uživatelé přístup a díky ní se dozví všechny postupy, které ke své práci potřebují.

2.6 SWOT MATICE

Na základě analýzy vnějšího a vnitřního okolí banky je zhotovena SWOT matice zobrazená v tabulce č. 5.

Tabulka č. 5 - SWOT Matice

	Silné stránky	**Slabé stránky**
Vnitřní prostředí	Informační systém umožňuje uživateli pracovat přímo v internetovém bankovnictví klienta	Informační systém neslouží jako jedno pracovní místo, uživatelé musí používat další aplikace a programy
	Nepřetržitý vývoj interně vyvinutého softwaru	
	Informační systém odpovídá strategii a organizační struktuře organizace	
	Informační systém umožňuje náhled na uživatele, kteří pracují na jednotlivých žádostech klienta	Informační systém neumožňuje uživateli náhled do mobilní aplikace klienta
	Informační systém umožňuje přímou kontrolu efektivity uživatelů	
Vnější prostředí	**Příležitosti**	**Hrozby**
	Možnost transferu technologií v rámci skupiny PPF	Bezpečnostní riziko - hrozba útoku na informační systém banky
		Operační riziko - hrozba podvodů uvnitř organizace
	Urychlení procesu schvalování úvěrů po zavedení nového informačního systému	Obtížná adaptace uživatelů na nový informační systém
		Objevení nových moderních technologií, na které banka nestačí reagovat

Podle výše uvedené SWOT matice vyplývá, že zavedení nového informačního systému, který by byl navržen jako jedno pracovní místo, by mohl zvýšit efektivitu práce zaměstnanců banky a podpořit firemní strategii, která se zaměřuje na budování vztahu s klienty. Vhodně navržený informační systém by také mohl snížit náklady na další vývoj informačního systému.

2.7 PROCES ZAVÁDĚNÍ INFORMAČNÍHO SYSTÉMU

S rozvojem společnosti a rychlým nárůstem počtu klientů vzniká potřeba urychlit práci v informačním systému, v programech a aplikacích s ním spojených. Proto je vhodné zavést v bance takový informační systém, který sloučí všechny programy a aplikace do jednoho prostředí, ve kterém zaměstnanci pracují. Výsledkem je nejen nákladová optimalizace, ale hlavně úspora pracovního místa, techniky, licencí a nákladů na klienta.

Proces zavádění informačního systému v bance má několik částí. Samotnému rozhodnutí, že dojde ke změně informačního systému, předchází mnoho porad a diskuzí vedoucích pracovníků. V následující části jsou uvedeny jednotlivé části procesu zavedení nového informačního systému v bance.

2.7.1 Stanovení požadavků na informační systém

Stanovení požadavků lze rozčlenit na tři druhy požadavků. Požadavky managementu specifikují, jaké nároky má business zadavatel na nový informační systém a jaké je jeho předběžné očekávání, případně z jakého důvodu chce nový informační systém zavést. Technické požadavky popisují, jak má být nový systém navržen, aby mohl být provozován na stávajících zařízeních a v systémech podniku. Nefunkční požadavky přímo nepodporují business cíle, ale jejich vliv na provoz informačního systému je velmi významná. V následující části jsou popsány základní požadavky, které by měl nový informační systém splňovat.

Požadavky managementu

- nákladová optimalizace,
- zlepšení efektivity práce uživatelů,
- nižší náklady na další vývoj informačního systému,
- úspora pracovního místa a sjednocení,
- přehlednější zobrazení informací o klientech,
- tvorba kvalifikovaného reportingu,
- uživatelská přívětivost informačního systému.

Technické požadavky

- databázový server,
- aplikační server,
- možnosti vzdáleného přístupu,
- počítačová síť,
- tiskárny,
- minimální konfigurace serverů,
- minimální konfigurace PC,
- stanice uživatelů.

Nefunkční požadavky

- zabezpečení – opatření proti kompromitování systému a útokům, zajištění důvěrnosti a integrity,
- výkonnost – doba reakce systému na uživatelův požadavek a počet transakcí provedených za určitý časový úsek,
- spolehlivost – zajištění integrity a konzistence aplikací i při zvýšeném zatížení,
- dostupnost – všechny služby a zdroje systému jsou neustále dostupné (vyjma nasazení patche apod.),
- rozšiřitelnost – možnost přidávání nových, nebo modifikace stávajících funkcionalit, aniž by byl systém negativně ovlivněn,
- udržitelnost – možnost opravení nedostatků systému, aniž by tím byla ovlivněn některý jiný systém.

2.7.2 Výběrové řízení na zhotovitele informačního systému

Zadavatel podle stanovených požadavků volí typ informačního systému, který chce implementovat. Poté osloví potenciální zhotovitele se svými požadavky včetně časového plánu, kteří buď nabídku přijmou a zúčastní se výběrového řízení, nebo odmítnou. Ve výběrovém řízení zadavatel posuzuje jednotlivé nabídky podle řešení standardních a zejména klíčových požadavků, cenové nabídky, garance záruky technické podpory, ochrany informací,

akceptace kritérií a dalších podrobnosti. Poté vybere zhotovitele informačního systému a stanovuje další detaily projektu.

2.7.3 Vytváření specifikací na informační systém

Po výběrovém řízení zadavatel se zhotovitelem informačního systému dopodrobna konzultuje specifikace na informační systém. Zjednodušeně, tyto specifikace říkají, jak přesně má informační systém fungovat. Specifikace lze rozdělit na tři stupně:

Business specifikace

Business specifikace stanovuje požadavky na informační systém z pohledu zadavatele. Jedná se o hrubý popis funkcí v informačního systému. Tyto specifikace podrobně řeší business analýza. Popisuje, jak má systém pracovat a jaké má koncový uživatel možnosti.

Požadavek zadavatele u telefonního kontaktu s klientem spočívá ve směrování hovorů. Ve chvíli, kdy klient volá do banky, následuje v několika vteřinách proces, který určuje přidělení hovoru operátorovi. Informační systém ověřuje, zda je dostupný last agent routing, tzn. operátor, se kterým klient řešil svůj požadavek naposledy. Pokud je tento operátor nedostupný, informační systém přiřazuje klienta jinému operátorovi. Jestliže není žádný operátor volný, klientovi je nabídnuto zpětné volání. Uživatel informačního systému si může klienta kdykoliv zpětně dohledat a zavolat mu.

U e-mailové komunikace s klientem jsou požadavky kladeny hlavně na to, jak může uživatel s e-mailem pracovat. To znamená, zda může e-mail přeposlat, odpovědět, nebo přeposlat a odpovědět, zda lze připojit přílohu apod. Stejně tak princip směrování e-mailů. Jeden z požadavků zadavatele je, aby klient svoje požadavky řešil nejlépe s jedním pracovníkem.

Zprávy do internetového bankovnictví technicky fungují stejně jako e-maily. Z pohledu uživatele je mezi těmito dvěma způsoby komunikace jediný rozdíl v tom, jaký typ informací může uživatel klientovi poskytnout. Vzhledem k tomu, že internetové bankovnictví je ověřený a zabezpečený komunikační kanál, může uživatel klientovi napsat veškeré podrobnosti o jeho účtu.

Business analýza

Business analýza řeší, jak předat informace o klientovi z databází a jiných systémů k uživateli prostřednictvím informačního systému. Vychází z business specifikace a popisuje

detaily spojení informačního systému s databázemi a ostatními integrovanými systémy. Jedná se například o zapisování a ukládání dat uživatelem, které databáze a informace jsou uživateli dostupné, na jaké systémy má dopad práce uživatele v informačním systému apod. Jeden z faktorů, který má vliv na zpřístupnění dat o klientovi, je přidělené oprávnění uživateli informačního systému. Díky těmto oprávněním může nahlížet do jednotlivých částí informačního systému a pracovat v nich. Další faktor je způsob komunikace uživatele s klientem. Pokud uživatel komunikuje telefonicky, má kompletní náhled a přístup na klientův účet a po ověření může se souhlasem klienta provádět aktivní operace na účtu. U ostatních typů komunikace s klientem má uživatel některé operace znemožněny.

Systémová analýza

Tato analýza řeší jednotlivé use cases business analýzy z pohledu dalšího vývoje. Zabývá se zejména hardwarovými a softwarovými požadavky na informační systém. Dále řeší, kteří uživatelé budou informační systém používat a na kterých serverech bude systém provozován. Systémová analýza popisuje, do kterých databází a jejich částí vedou jednotlivé složky informačního systému a jak se mají při zadání požadavku zachovat, aby byly poskytnuty požadované informace uživateli, který má k těmto datům přístup.

2.7.4 Vytváření návrhu

Při vytváření návrhu spolupracuje zhotovitel informačního systému s business analytikem a solution architektem zadavatele. V projekční části vytváření návrhu zhotovitel analyzuje požadavky zadavatele a společně stanoví způsob realizace. V technické části vytváření návrhu zadavatel ověřuje funkčnost stanovených požadavků v projekční části. Ve fázi implementace je systém na základě výstupů z projekční a technické části vytvořen, a následně předán na testování.

Projekční část

Projekční část vytváření návrhu představuje vytvoření dokumentu, který upřesňuje cíle projektového záměru, popisuje návrh business procesů a pracovních postupů, určuje rozsah systému ve formě seznamu funkcí, integračních požadavků a architektonických a provozních omezení. Tento dokument by měl zahrnovat také analýzu rizik, pro které jsou navržena eliminační opatření, případně metody pro snížení jejich dopadu. V tomto případě bude použita analýza způsobů, důsledků a kritičnosti poruch (FMECA), ve které jsou stanovena rizika pro jednotlivé procesy a subprocesy. Dále je vytvořen časový plán a detailní rozpočet

implementace po jednotlivých složkách. Časový plán představuje podrobný časový harmonogram s očekávaným datem dokončení projektu.

Návrh informačního systému by měl zahrnovat řešení nároků s požadovanými business funkcemi a jejich detailní specifikaci. Vytváří se veškeré potřebné modely business procesů, funkčností, zpracování a uložení dat a návrh testovacích prostředí, která budou využívána v procesu testování. Jednotlivé funkčnosti jsou zařazeny do kategorií. Nakonec se vytváří architektura systému.

Technická část

V technické části návrhu je popsán detailní technický a funkční návrh implementace, který by měl odpovídat rozsahu a potřebám odsouhlaseným v dokumentu projekční části návrhu. Výstupem technické části je prototyp, na kterém zadavatel ověřuje vybrané, zejména specifické funkčnosti, vzhled a další technické vlastnosti. V rámci technického návrhu je stanoven datový model, architektura řešení, infrastruktura, standardy a návrhy uživatelského prostředí. V technické dokumentaci jsou stanoveny plány a strategie:

- vývoje modulů a částí informačního systému,
- testování,
- systémové integrace,
- zavedení informačního systému,
- provozu a správy informačního systému.

2.7.5 Implementace

Do této fáze vstupují jasně vymezené specifikace funkčností a technologické způsoby jejich realizace. Zhotovitel spolu s interními vývojáři vytváří informační systém, který pak předává na testování.

2.7.6 Testování

Proces testování lze rozdělit na čtyři fáze.

Vytváření test cases

V první fázi se vytváří test cases, které jsou připravovány podle požadavků systémové analýzy. Testeři vytváří testovací scénáře, ve kterých je stanoveno, jak otestovat jednotlivé funkce, aby splňovaly požadavky systémové analýzy.

Akceptační testy

V druhé fázi se provádí akceptační testy v jednotlivých prostředích. Zjišťuje se, zda je dané prostředí funkční, a pokud ano, spouští se další fáze testů

Testy funkčních požadavků

Třetí fáze zahrnuje provádění testů funkčností systému. Testy jsou prováděny v následujících prostředích:

- DEV prostředí – jedná se o vývojové testování, jehož cílem je nastavení systému podle předem daných specifikací. Vývojáři používají agilní metody, které umožňují rychlý vývoj a zároveň umožňují reagovat na změnu požadavků v průběhu vývojového cyklu. Vývojářské činnosti jsou prováděny po malých částech do jednotlivých balíků.
- INT prostředí – zde se sbírají všechny dovyvinuté balíky z DEV prostředí a ladí se nové funkcionality jako celek. Jedná se o kompletní testovací prostředí, kde se testuje, zda jsou všechny části kompatibilní.
- UAT prostředí – zkratka UAT znamená User Acceptance Testing, tedy uživatelské akceptační testování. Informační systém je testován jako celek a přímo souvisí s business specifikací. Cílem je objevit chyby které nebyly nalezeny na INT prostředí a objevily se až při kompletní implementaci. Po testování na UAT prostředí se provádí rozšířená akceptační kritéria. Testují se vlastnosti systému, kterých se nové funkcionality přímo netýkají, za účelem zjištění případných chyb v ostatních částech systému.
- PERF prostředí - PERF test ověřuje schopnost systému zvládnout velké množství současně pracujících uživatelů a spouštěných programů. Pokud test neprojde, spočívá řešení nejdříve v ladění systému a teprve poté v navýšení hardwaru. Aby byl test plně vypovídající, je třeba ho provést na HW, který je konfigurací obdobný jako v produkčním prostředí. Může zahrnovat jak

kvantitativní testy, tak kvalitativní testy. Při testování výkonnosti se zároveň zjišťuje, jestli systém splňuje požadované specifikace.

- PREPROD prostředí - PREPROD je zkratka z pre-production testing. Předprodukční prostředí by mělo být co nejvíce totožné s produkčním prostředím. Údaje, které jsou v předprodukčním prostředí použity, jsou reálná data o klientech. Použití těchto dat ale nemá na klienty žádný vliv. Pokud se v těchto testech neopraví všechny chyby, pak jsou dále do produkce dodávány pomocí balíků.

Testy nefunkčních požadavků

Čtvrtá část testování zahrnuje provádění nefunkčních testů. Jedná se o následující testy:

- Penetrační testy – cílem penetračního testu je najít slabá místa v systému, která by mohl najít potenciální útočník. Jedná se o simulaci útoku, kde jednotlivé kroky testování jsou měněny podle aktuálních zjištění.
- Zátěžové testy – zátěžové testy jsou prováděny v PERF prostředí a zjišťují, jaká je odezva informačního systému na velký počet různých požadavků. Tím lze vysledovat, ve které části systému je zapotřebí provést optimalizaci.
- SQL injection – jedná se o techniku napadení databázové vrstvy programu vsunutím kódu přes neošetřený vstup a vykonání vlastního pozměňujícího a poškozujícího SQL příkazu. Tento neošetřený postup vzniká při propojení aplikační vrstvy s databázovou vrstvou.

V procesu vytváření návrhu je stanoven plán testování, ve kterém jsou definována jednotlivá testovací prostředí, ve kterých bude informační systém testován. Plán testování obsahuje další informace o tom, jak bude testování probíhat. Jedná se zejména o:

- cíle a požadavky testování projektu,
- rozsah testování,
- typy testování,
- nástroje pro provádění a řízení testů,
- pokrytí business požadavků,
- kritéria úspěšnosti testovacích scénářů,

- testovací prostředí,
- testovací data,
- role a zodpovědnosti.

2.7.7 Nasazení informačního systému

Před nasazením nového informačního systému banka zajišťuje, aby oprávnění uživatelé byli schopni s informačním systémem pracovat tak, aby klienti nepoznali změnu. Zároveň definuje krizové scénáře včetně návratových scénářů. Teprve potom započne proces nasazení, na jehož konci je oprávněný uživatel schopný pracovat v novém informačním systému.

Příprava

Při vytváření návrhu se stanovuje očekávaný termín nasazení nového informačního systému, který může být výrazně odlišný od konečného termínu. Před stanovením konečného termínu je nutné, aby byli oprávnění uživatelé dostatečně proškolení. Nejefektivnější způsob, jak mohou uživatelé získat znalosti o novém informačním systému, je jejich aktivní účast na konečné fázi jeho vytváření. Vybraná skupina uživatelé se učí pracovat v novém informačním systému v pilotním režimu. Ne všichni se však pilotního režimu mohou zúčastnit, a tak vedení banky musí zajistit školení pro všechny oprávněné uživatele a vytvořit uživatelskou dokumentaci, kterou budou mít uživatelé přístupnou.

Definování krizových scénářů

Před nasazením informačního systému banka definuje krizové scénáře. Zajišťuje minimální konfiguraci informačního systému, aby v případě neúspěšného nasazení fungoval původní systém. Pokud selže i původní systém, banka musí být schopna zajistit klientovi základní servis.

Pro eliminaci rizik spojených s nasazením informačního systému do produkčního prostředí je nutné naplánovat a připravit:

- migrační plán,
- pilotní režim.

Migrační plán popisuje všechny kroky zavedení informačního systému do produkčního provozu, tzv. roll-out. Cílem této fáze je spustit informační systém pro všechny

oprávněné uživatele. Podle složitosti nasazovaného systému je nutné počítat s případy, kdy může během migrace dojít k neplánovaným technickým problémům. Proto se připravují postupy návratových scénářů, tzv. roll-back, včetně zajištění zdrojů pro migraci. Tyto návratové scénáře umožňují vrátit se do předchozího stavu, od kterého lze pokračovat v instalaci a dokončení migrace. Migrační plán popisuje jednotlivé kroky migrace, dopady na okolní integrované systémy, návratové scénáře, komunikační plán se seznamem účastníků migrace, pomigrační režim a seznam rizik. Samotný migrační plán eliminuje rizika, protože je dopředu stanoveno, co a kdy se má během migrace provést pro úspěšné zavedení informačního systému.

Před zavedením informačního systému do produkčního prostředí je z důvodu eliminace rizik a zajištění stability zaveden pilotní režim. Vybraná skupina uživatelů zkouší pracovat v novém informačním systému, který je spuštěn v produkčním prostředí. Tím se eliminují rizika související se spuštěním informačního systému pro všechny oprávněné uživatele. Při instalaci systému do pilotního režimu se zároveň ověří migrační postupy včetně návratových postupů, a tím se eliminují rizika produkční migrace. Součástí pilotního režimu je ověření funkcí a výkonnostních parametrů.

Odstávka

Odstávka probíhá podle časového harmonogramu v nočních hodinách tak, aby využívání bankovních služeb klienty bylo co nejméně omezeno. Klientovi není umožněno přihlásit se do svého internetového bankovnictví, může ale vybírat z bankomatu a platit kartou. Všechny transakce jsou ověřovány v takzvaném offline režimu.

V této části je informační systém zcela připraven k nasazení. Dokončuje se nasazení a spuštění systému. Po ukončení nasazení je proveden smoke test. Tento test se provádí bezprostředně po nasazení informačního systému do produkčního prostředí. Nejdříve informační systém testují testeři a vývojáři. V případě jakýchkoliv chyb se testeři obrací na odpovědné osoby, které jsou součástí týmu a přítomné v době nasazování. Prochází se celý systém, chyby a nefunkčnosti, pokud je vše v pořádku, odstávka je ukončena.

Provoz

V této fázi, po ukončení odstávky, je umožněno všem oprávněným uživatelům používat nový informační systém. Pokud uživatelé nejsou schopni informační systém v produkčním prostředí spustit, pokračují v práci v původním systému a provádí se roll-back

podle návratového scénáře. Roll-back je nejhorší možný výsledek nasazení nového informačního systému, a v případě, že musí být proveden, stanovuje se další termín pro nasazení. V případě úspěšného nasazení uživatelé hlásí chyby helpdesku a vedoucím pracovníkům.

2.7.8 Odstranění chyb

V této části se odstraňují chyby, které se vyskytly v produkčním prostředí, ale v testování nikoliv. Určuje se priorita jednotlivých chyb. Nejprve se pracuje na odstranění chyb s nejvyšší prioritou. Ostatní chyby jsou evidovány a opravují se v plánovaných odstávkách, nebo, v případě drobných chyb, za provozu. Pokud jsou chyby na straně zhotovitele, chyby se odstraňují při dalším nasazení aktuální verze. Cílem je zajistit plynulý provoz banky tak, aby klient nepoznal změny a mohl bez větších omezení využívat služeb banky. V závislosti na tom, o jaké chyby se jedná, odstraňují chyby interní vývojáři a pracovníci aplikační podpory

2.7.9 Akceptace projektu

Cílem převzetí informačního systému do provozní správy je zajištění efektivního provozu a dlouhodobého rozvoje systému. Před ukončením projektu pracovníci provozu řeší následující úkoly:

- převzetí dokumentace k informačnímu systému,
- zajištění konzultací a technické podpory s pracovníky projektu,
- seznam chyb a jejich řešení,
- seznam řešených chyb v testech,
- akceptační protokoly testů,
- převzetí funkční instalace,
- převzetí zdrojových kódů,
- postupy instalace do jednotlivých prostředí,
- postupy zálohování a obnovy,
- konfigurace testovacího a vývojového prostředí.

Výstupem procesu převzetí systému z projektu do provozní správy je protokol o převzetí. Zhotovitel informačního systému dodá zadavateli další protokoly jako jsou

akceptace testů, akceptace dokumentace, akceptace pilotního režimu, akceptace migrace do produkce a akceptace převzetí. Tímto se projekt uzavírá v rámci zavedení informačního systému. V tuto chvíli pracovníci provozní správy přebírají odpovědnost za správu informačního systému v produkčním prostředí.

2.8 HODNOTÍCÍ TABULKY FMECA

V analýze FMECA je prováděno hodnocení pravděpodobnosti výskytu poruchy, klasifikace závažnosti a pravděpodobnost včasného odhalení poruchy.

Pro stanovení pravděpodobnosti výskytu byla stanovena stupnice 1 až 5, přičemž 1 klasifikuje poruchu jako nepravděpodobnou a 5 jako téměř nevyhnutelnou. Ve formuláři FMECA je pravděpodobnost výskytu označena písmenem O (z anglického occurrence). Klasifikační stupnice je zobrazena v tabulce č. 6.

Tabulka č. 6 - Hodnocení pravděpodobnosti výskytu

Číselné hodnocení	Četnost výskytu	Příklad
1	Nepravděpodobný výskyt	Porucha je nepravděpodobná
2	Velice slabý výskyt	Poměrně málo poruch
3	Občasný výskyt	Občasné poruchy
4	Pravděpodobný výskyt	Opakující se poruchy
5	Četný výskyt	Porucha je téměř nevyhnutelná

Pro klasifikaci závažnosti bylo použito hodnocení na stupnici 1 až 5, přičemž 1 značí pro projekt nevýznamnou závažnost a 5 katastrofickou závažnost. Ve formuláři FMECA je závažnost nebezpečí označena písmenem S (z anglického severity). Klasifikační stupnice je zobrazena v tabulce č. 7.

Tabulka č. 7 - Hodnocení úrovně závažnosti

Číselné hodnocení	Úroveň závažnosti	Příklad
1	Nevýznamná	Žádný zjistitelný důsledek, neshoda s požadavky je méně než 10%
2	Okrajová	Důsledek je zjistitelný, neshoda s požadavky je méně než 25%, ale uživatel poruchu nerozpozná
3	Významná	Objekt je ve většině případů provozuschopný, ale technické parametry jsou sníženy, uživatel rozpozná poruchu, neshoda s požadavky více než 25%
4	Velmi závažná	Vysoká klasifikace závažnosti, je ovlivněna provozuschopnost objektu nebo dojde ke ztrátě základní funkce, potenciální způsob poruchy na sebe upozorňuje
5	Kritická	Velmi vysoká klasifikace závažnosti, potenciální způsoby poruchy na sebe neupozorňuje varováním, ztráta základní funkce, ztráta dat

Pro hodnocení pravděpodobnosti detekce byla použita klasifikační stupnice 1 až 5, přičemž 1 znamená vysokou pravděpodobnost odhalení a 5, že odhalení je absolutně nejisté. Ve formuláři FMECA je závažnost nebezpečí označena písmenem D (z anglického detection). V tabulce č. 8 je zobrazena klasifikační stupnice pro hodnocení.

Tabulka č. 8 - Hodnocení pravděpodobnosti včasné detekce

Číselné hodnocení	Detekce	Příklad
1	Velmi vysoká	Při řízení návrhu je vysoká naděje, že potenciální mechanismus a následný způsob poruch bude odhalen
2	Středně vysoká	Je středně vysoká naděje, že potenciální mechanismus a následný způsob poruchy bude odhalen
3	Nízká	Je malá naděje, že při řízení návrhu bude potenciální příčina a následný způsob poruch odhalen
4	Velmi slabá	Je velmi malá naděje, že při řízení návrhu bude potenciální příčina a následný způsob poruch odhalen
5	Absolutně nejistá	Při řízení návrhu není možné odhalit potenciální příčinu a následný způsob poruch

Na základě těchto hodnocení, která jsou provedena odhadem, je součinem vypočteno číslo priority rizika (RPN – risk priority number). Vzhledem k tomu, že číslo RPN u jedné poruchy s průměrnými hodnotami může být vyšší než u jiné poruchy s velmi vysokou závažností, ale nízkou pravděpodobností výskytu a odhalení, slouží RPN spíše pro lepší

proces rozhodování, aby se se samotným číslem RPN posuzovala i třída závažnosti způsobu poruch.

V této analýze FMECA jsou stanovena současná a doporučená opatření pro všechna identifikovaná nebezpečí. Detailní slovní popis nebezpečí a navrhovaných opatření je proveden pouze pro ta nebezpečí, jejichž závažnost je kritická.

2.9 IDENTIFIKACE NEBEZPEČÍ

V této části práce je provedena identifikace nebezpečí, jejich příčin a následků u jednotlivých procesů zavádění informačního systému. Tyto procesy jsou dále rozděleny na subprocesy tak, jak je uvedeno v popisu zavádění informačního systému. Dále je stanovena pravděpodobnost výskytu, úroveň kritičnosti a pravděpodobnost včasné detekce těchto nebezpečí. Z těchto čísel je vypočtena hodnota RPN.

U nebezpečí, jejichž kritičnost je ohodnocena číslem 5, je věnována největší pozornost. Následek těchto nebezpečí může být až kritický. Tato nebezpečí mohou znemožnit nasazení nového informačního systému, způsobit významnou finanční ztrátu, ztrátu dat a interních informací, poškození zdraví a ohrožení na životě, porušení legislativy případně ohrozit další fungování podniku.

2.9.1 Stanovení požadavků na informační systém

Proces stanovení požadavků na informační systém zahrnuje tři subprocesy. Identifikovaná nebezpečí jsou uvedena v tabulkách č. 9, 10 a 11..

Tabulka č. 9 – Požadavky managementu

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Nedostatečný budget na zhotovení IS	Neočekávané investice do jiných projektů, strategické rozhodnutí	Nenalezení zhotovitele IS, který by přijal finanční nabídku, nebo oslovení nevhodných zhotovitelů	2	**5**	1	10
Nereálné očekávané přínosy	Přeceňování technických prostředků bez zajištění přiměřených odpovídajících procesů, přeceňování návratnosti investice, která není vždy vyčíslitelná	Negativní postoj k dalším investicím do ICT nebo naopak další přemrštěné investice	4	4	4	64
Stanovení krátkého časového limitu na projekt	Nereálný odhad doby trvání projektu, nedostatečná příprava podkladů a spolupráce projektového týmu s ostatními pracovníky podniku	Zvýšení nákladů na IS, odmítnutí projektu zhotovitelem, prodloužení doby interního vývoje	5	4	5	100

V této části je identifikováno jedno nebezpečí, jehož úroveň kritičnosti je hodnota 5. Pokud vedení podniku vymezí na projekt nedostatečný budget, hrozí velké riziko, že žádný z oslovených zhotovitelů nebude mít o zakázku zájem. V horším případě by o projekt projevil zájem nevhodný nebo nezkušený zhotovitel. Výsledný implementovaný informační systém by představoval významnou investici, která by byla vyčíslována ve ztrátách, nikoliv v zisku.

Opatřením může být žádost o úvěr, nebo nalezení vhodného investora, který by tento projekt podpořil. Vzhledem k tomu, že Air Bank je součástí finanční skupiny PPF, jsou obě tyto možnosti nikoliv krajním řešením, ale naopak příležitostí pro získání lepších podmínek financování projektu.

Tabulka č. 10 – Stanovení technických požadavků

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Opomenutí některého z technických požadavků na IS	Chyba vedoucího IT infrastructure	Zvýšení nákladů na provoz na technické vybavení, dodatečné změnové požadavky na IS	1	4	5	20
Chybná specifikace technických požadavků	Chyba vedoucího IT infrastructure	Zvýšení nákladů na provoz na technické vybavení, dodatečné změnové požadavky na IS	1	4	5	20

U žádného nebezpečí v tomto subprocesu nedosáhla úroveň kritičnosti hodnoty 5. Všechna navrhovaná opatření jsou uvedena v přílohách.

Tabulka č. 11 – Stanovení nefunkčních požadavků

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Opomenutí některého nefunkčního požadavku	Chyba vedoucího IT security	IS postrádá důležité vlastnosti, zvýšení nákladů, prodloužení doby interního vývoje, IS nepředstavuje konkurenční výhodu a návratnost investice neodpovídá očekávané	2	**5**	5	50
Nepřesná specifikace jednotlivých požadavků	Chyba vedoucího IT security	IS postrádá důležité vlastnosti, zvýšení nákladů, prodloužení doby interního vývoje, IS nepředstavuje konkurenční výhodu a návratnost investice neodpovídá očekávané	2	**5**	5	50

U obou identifikovaných nebezpečí byla stanovena úroveň kritičnosti hodnotou 5. Opomenutí některého z nefunkčních požadavků, nebo jejich nepřesná specifikace způsobí, že implementovaný systém bude postrádat důležité vlastnosti na zabezpečení, výkonnost, dostupnost, rozšiřitelnost a další požadované vlastnosti. Tyto nedostatky mohou být objeveny ve kterékoliv fázi zavádění informačního systému, a čím později jsou objeveny, tím větší budou mít změnové požadavky vliv na výslednou cenu projektu, která může být díky těmto změnám více než dvojnásobná. Pokud se zadavatel rozhodne, že projekt akceptuje tak, jak byl vytvořen, je pravděpodobné, že návratnost této investice bude velmi nízká, reálné přínosy nebudou odpovídat očekávaným, a nový informační systém se stane spíše zátěží pro pracovníky. V případě opomenutí některého z bezpečnostních prvků může dojít k úniku informací a ztrátě dat.

Opatření, která jsou navržena, spočívají ve stanovování požadavků podle metodiky ITIL (Information Technology Infrastructure Library), která představuje rámec best practice s pomocí kterého dosáhne podnik požadované kvality IT služeb a překoná překážky související s rozvojem vlastního informačního systému.

2.9.2 Výběrové řízení na zhotovitele informačního systému

Proces výběrové řízení na potenciálního zhotovitele informačního systému zahrnuje dva subprocesy. Identifikovaná nebezpečí jsou uvedena v tabulkách č. 12 a 13.

Tabulka č. 12 – Oslovení potenciálních zhotovitelů

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Nezájem zhotovitelů o zakázku	Nedostatek času a/nebo kapacity oslovených zhotovitelů	Prodloužení doby výběrového řízení z důvodu nedostatku zájemců o projekt	4	**5**	1	20
Oslovení nesprávných zhotovitelů	Nedostatek zhotovitelů IS na trhu, zadavatel nemá dostatek informací o všech potenciálních zhotovitelích	Nevyhovující návrh od potenciálního zhotovitele	4	4	1	16

V tomto suprocesu bylo stanoveno kritické nebezpečí nezájem zhotovitelů o zakázku. Pokud by vedení podniku dospělo k závěru, že je nutné zavést nový informační systém, který přispěje k dalšímu rozvoji, vymezilo pro nový informační systém dostatečný budget, a přesto by o tento projekt žádný z oslovených zhotovitelů nejevil zájem, management řeší významný problém. Na rozdíl od státních zakázek nemůže vypsat veřejné výběrové řízení nebo tendr, protože informace, že se bude zavádět nový informační systém, je interního charakteru. Podnik si samozřejmě může ponechat stávající informační systém, případně zakoupit nějaký univerzální podnikový informační systému typu ERP (Entrerprise Resource Planning), CRM (Customer Relationship Management), ale opět zde hrozí riziko, že tento typ informačního systému bude pro banku nevhodný a investice bude ztrátová.

Opatření, která jsou navržena, spočívají v oslovení těch zhotovitelů, kteří jsou opravdu schopni splnit požadavky zadavatele, a počkat se zavedením nového informačního systému do doby, než tento zhotovitel bude mít na projekt čas a kapacitu.

Tabulka č. 13 – Výběrové řízení

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Nepřihlásí se žádný zhotovitel	Oslovení zhotovitelé nedokážou vyhovět požadavkům na IS nebo je pro ně nabídka finančně nezajímavá	Prodloužení doby výběrového řízení z důvodu nedostatku zájemců o projekt	3	**5**	1	15
Zmanipulování výběrového řízení	Korupce	Výběr nevhodného zhotovitele, nový IS nepřispívá k získání konkurenční výhody a/nebo růstu tržeb a dalších očekávaných přínosů	2	**5**	5	50
Výběr špatného zhotovitele	Nedostatečný budget na zhotovení informačního systému a/nebo nevyjasnění si specifických požadavků na IS se zhotovitelem	Zvýšení nákladů na další rozvoj IS, projekt nevede k očekávané ekonomické efektivnosti	4	**5**	5	100
Licenční omezení	V nabídce zhotovitele jsou uvedeny podmínky pro zakoupení dalších licencí, které nejsou započteny do konečné ceny projektu	Překročení budgetu	4	4	5	80

V tomto subprocesu byly stanoveny tři nebezpečí s nejvyšším hodnocením kritičnosti. Opět se opakuje, že žádný ze zhotovitelů nebude mít o zakázku zájem, tentokrát z důvodu neschopnosti vyhovět požadavkům na informační systém, nebo protože je pro ně nabídka finančně nezajímavá. Jak bylo již uvedeno v části stanovení požadavků na informační systém, nedostatečný budget lze vyřešit úvěrem nebo investorem, který projekt podpoří. Pokud ale zadavatel informačního systému stanoví takové požadavky, které žádný z oslovených zhotovitelů nedokáže splnit, nejspíš stanovil příliš specifické požadavky, které by se daly řešit přizpůsobením funkcím informačního systému, případně tato specifika konzultovat se zhotovitelem. V opačném případě se výběrové řízení bude stále prodlužovat a výsledek bude nejasný.

Opatření, které je navrženo, spočívá v navýšení budgetu a přehodnocení těch požadavků, které oslovení zhotovitelé nejsou schopni dodržet.

Další kritické nebezpečí je zmanipulování výběrového řízení formou korupce. Výsledkem může být výběr nesprávného zhotovitele, jehož implementovaný systém nebude plnit očekávání a opět se projekt bude vyčíslovat spíše ve ztrátách. Toto nebezpečí může být odhaleno ve kterékoliv fázi procesu, nebo nikdy.

Opatřením může být takové výběrové řízení, kde bude o zhotoviteli nového informačního systému rozhodovat více členů, jejichž hlasy budou mít stejnou váhu. Pokud pro nového zhotovitele nebude hlasovat více než 60% členů, budou probíhat další kola výběrového řízení, dokud skupina nevybere nejvhodnějšího zhotovitele.

Dalším kritickým nebezpečím je výběr nevhodného zhotovitele informačního systému. Zadavatel může vybrat nevhodného zhotovitele proto, že tým, který zhotovitele vybírá, není sestaven z odborníků na informační systémy, a že se výběrového řízení neúčastní vrcholový management. Prezentující člen potenciálního zhotovitele by měl zadavateli poskytnout úplné a pravdivé informace o svých službách. Opět zde také figuruje nedostatečný budget na zhotovení informačního systému, kvůli kterému by vhodní zájemci o projekt mohli dát přednost jiným zakázkám.

Účinné opatření je ověření si referencí vybraného zhotovitele systému u jiných firem, ve kterých systém implementoval. Je vhodné se zajímat o celý proces návrhu informačního systému, samotnou implementaci, poskytnutí technické podpory, zhotovení a včasné dodání dokumentace, jestli jim nový systém přinesl očekávaný užitek apod.

2.9.3 Vytváření specifikací na informační systém

Proces vytváření specifikací na informační systém se skládá ze tří subprocesů. Identifikovaná nebezpečí jsou uvedena v tabulkách č. 14, 15 a 16.

Tabulka č. 14 – Business specifikace

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Nepřesnosti v popisu jednotlivých procesů	Nepoužívání business slovníku	Řešitel business požadavků nemusí všechny požadavky pochopit správně	5	3	1	15
Opomenutí části procesu	Chyba business analytika	Zvýšené provozní náklady, prodloužení doby projektu	2	3	4	24
Zjednodušení procesu	Business analytik nedefinuje proces detailně	Prodloužení doby návrhu	3	3	4	36

U žádného nebezpečí v tomto subprocesu nedosáhla úroveň kritičnosti hodnoty 5. Všechna navrhovaná opatření jsou uvedena v přílohách.

Tabulka č. 15 – Business analýza

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Špatně popsaná procesní napa	Solution architekt nedefinuje proces detailně	Prodloužení doby návrhu, zhotovitel neporozumí zadání IS	4	3	3	36
Vytváření zbytečných procesů navíc	Nedostatečné množství schůzek solution architekta se zadavatelem a zhotovitelem	Prodloužení doby návrhu, zvýšení nákladů na projekt	2	3	3	18

U žádného nebezpečí v tomto subprocesu nedosáhla úroveň kritičnosti hodnoty 5. Všechna navrhovaná opatření jsou uvedena v přílohách.

Tabulka č. 16 – Systémová analýza

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Opomenutí bezpečnostních opatření jednotlivých databází a systémů	Nedostatečné testování zabezpečení těchto databází a systémů	Prodloužení doby testování, zvýšené náklady, možnost napadení systémů	1	**5**	5	25
Chybné stanovení propojení IS s jednotlivými databázemi	Chyba solution architekta	IS neposkytne požadované informace uživateli	1	**5**	5	25

V tomto subprocesu byly dvě nebezpečí stanovena jako kritická. Pokud by došlo k opomenutí bezpečnostních opatření jednotlivých systémů, prodloužila by se doba testování a tím i výsledná cena projektu. Otázkou zůstává, zda by se v procesu testování přišlo na všechny opomenutá bezpečnostní opatření. Pak by hrozilo napadení systému a ztráta dat.

Opatření, které toto nebezpečí sníží, je sestavit tým složený z bezpečnostních inženýrů a analytiků, kteří se budou podílet na zajištění bezpečnostních opatření. Jakmile dojde k otestování zabezpečení, měla by být provedena další kontrola těchto opatření.

Dalším kritickým nebezpečím je chybné propojení informačního systému s jednotlivými databázemi. Návrh na propojení provádí solution architekt. Pokud by na základě návrhu došlo k chybnému propojení informačního systému s databázemi, informační systém neposkytne uživateli požadované informace. Na tuto chybu v propojení by pravděpodobně přišli testeři. I ti ale mohou opomenout otestovat všechny funkčnosti. V takovém případě by byl nasazený informační systém nefunkční.

Řešením může být udělení přístupu všem oprávněným osobám do dokumentace, kde je popsaná architektura systému. Tento přístup může sloužit jako kontrola navrženého propojení informačního systému s jednotlivými databázemi.

2.9.4 Vytváření návrhu

Proces vytváření návrhu je rozdělen na dva subprocesy. Identifikovaná nebezpečí jsou uvedena v tabulkách č. 17 a 18.

Tabulka č. 17 – Projekční část

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Vytvoření nereálného časového plánu pro zavedení IS	Chyba projekt managementu	Prodražení a prodloužení očekávané doby zhotovení IS	5	4	5	100
Nevytvoření všech potřebných testovacích prostředí	Chyba test designera nebo test managera	Nemožnost otestování všech funkcí IS	5	2	5	50
Rozpočet nezahrnuje všechny nákladové položky IS	Zhotovitel zatají některé zpoplatněné služby, které jsou součástí IS, např. přístupy, programové úpravy, hotline apod.	Výsledná cena je odlišná	4	4	5	80
Chyba v návrhu business procesů	Chyba business analytika	Prodloužení doby vytváření návrhu, chyby v testování	2	4	5	40
Analýza rizik je vytvořena později než v návrhové části projektu nebo vůbec	Expertní tým, který analýzu provádí, nemá čas na včasné provedení analýzy, projekční tým nepřikládá analýze rizik dostatečnou důležitost	Prodloužení a prodražení projektu, neúspěšné dokončení, nedostatečné zabezpečení IS, ztráta dat o klientech	4	**5**	1	20

Kritickým nebezpečím je vytvoření analýzy rizik později než v návrhové části projektu, nebo nezhotovení analýzy rizik. Nejhorším možným následkem je jakékoliv opomenuté hrozby, neúspěšné dokončení nasazení nového informačního systému, nedostatečné zabezpečení, finanční ztráty, ztráta dat o klientech apod. Analýza rizik je většinou zpracována expertním týmem v případě, že na to mají jednotliví členové týmu čas. Z toho plyne, že projekční tým nepřikládá analýze rizik dostatečnou důležitost.

Řešením je zajištění expertního týmu ještě před výběrovým řízením, průběžná kontrola a doplňování položek do analýzy rizik, a hlavně vymezení času pro zhotovení této analýzy. Pokud management není schopen složit tým z expertů, kteří by analýzu rizik

provedli, může oslovit společnost, která analýzu rizik zhotoví. Pokud bude analýza rizik prováděna externě, je nutné s danou společností uzavřít smlouvu o mlčenlivosti.

Tabulka č. 18 – Technická část

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Chyby v datovém modelování	Chyba vývojáře	Při práci v systému se zobrazí chyba, nebo se nezobrazí data, nebo je systém úplně nefunkční	2	**5**	1	10
Uživatelské prostředí vznikne až na základě datového modelu	Chyba designer vývojáře	V uživatelském prostředí nebudou všechny informace, které uživatel potřebuje, nebo jich bude zbytečně moc a systém se zpomaluje	2	2	1	4

V technické části procesu vytváření návrhu můžou být chyby v datovém modelování kritické. Toto nebezpečí může být objeveno ve kterékoliv části projektu. Vývojář by měl mít k dispozici vždy návrh business analytika, který mu datové modelování usnadní. Pokud by se vyskytly chyby v datovém modelování, informační systém by nebyl pro uživatele plně dostupný. Při zadání požadavku se můžou zobrazovat chyby, nezobrazí se požadovaná data, nebo je systém úplně nefunkční.

Opařením proti tomuto nebezpečí může být poskládání systému z jednotlivých modulů tak, aby tyto moduly byly na sobě co nejméně závislé. Ve chvíli, kdy se v jednom modulu vyskytne chyba, ostatní moduly mohou fungovat korektně.

2.9.5 Implementace

Proces implementace není rozdělen na další subprocesy. Identifikovaná nebezpečí jsou uvedena v tabulce č. 19.

Tabulka č. 19 - Implementace

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Opomenutí uživatelských požadavků na IS	Nedostatečná zainteresovanost pracovníků banky na procesu zavádění IS	Změna zadání, změna časového harmonogramu, prodražení projektu	3	**5**	3	45
Naprogramované uživatelské řešení odpovídá odsouhlasené analýze, ale ne představě zadavatele IS	Nepotvrzování si jednotlivých částí požadavků se zhotovitelem, nedostatečná zainteresovanost pracovníků banky na projektu	Dodatečné požadavky funkčností nad rámec analýzy, změna časového harmonogramu, prodražení projektu	5	**5**	3	75
Chyby v migraci dat	Neodsouhlasení architektonických struktur, špatné naprogramování převodového můstku, neočištění dat před převodem	Chyba vývojáře	2	4	1	8

V procesu implementace se vyskytují dvě nebezpečí s kritickým hodnocením závažnosti. Pokud zhotovitel nebo zadavatel opomene některé uživatelské požadavky na informační systém, musí se změnit nastavení pomocí změnových požadavků. Tím se také prodlužuje časový harmonogram a výsledná cena projektu se navyšuje. Příčinou tohoto opomenutí nejčastěji bývá nedostatečná zainteresovanost pracovníků banky na procesu návrhu a implementace nového informačního systému. Problém spočívá v tom, že pracovníci podniku tyto činnosti provádí většinou nad rámec vlastních úkolů a stávají se pro ně spíše dlouhodobou přítěží.

Nebezpečí, kdy naprogramované uživatelské řešení odpovídá odsouhlasené analýze, ale ne představě zadavatele, úzce souvisí s opomenutím požadavků na informační systém. Příčinou je také to, že si zadavatel a zhotovitel nepotvrzují jednotlivé části požadavků v průběhu vytváření návrhu a implementace. Všechny požadavky, které zadavatel má, by měly být rozřazeny do kategorií kritické, významné a nepodstatné. Dokud zhotovitel zejména kritické požadavky nesplní dokonale, měl by jej zadavatel považovat za nesplněný požadavek.

Řešením těchto dvou situací je zajištění dostatečného množství kompetentních pracovníků podniku na stanovování požadavků a celém procesu zavádění informačního systému.

2.9.6 Testování

Proces testování je rozdělen na čtyři subprocesy. Identifikovaná nebezpečí jsou uvedena tabulkách č. 20, 21, 22 a 23.

Tabulka č. 20 – Vytváření test cases

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Nepopsání testovacího scénáře v úplném rozsahu	Nedostatek času, chyba testera	Špatně provedené regresní testy (následující kolo testů nemusí odpovídat požadovaným výsledkům)	4	1	1	4
Business zadavatel mění požadavky na systémovou analýzu v průběhu testování	Časté změny v business analýze	Prodloužení doby testování	5	4	2	40
Testovací scénáře neodpovídají požadavkům systémové analýzy	Chyba v komunikaci mezi testery a analytiky	Špatná funkčnost systému	5	1	1	5
Špatné výsledky úspěšnosti testů	Chyba testera	Možné prodloužení doby testování, s těmito chybami se počítá	5	1	1	5
Nevytvoření všech možných test cases	Chyba testera	Nedostatečné otestování	5	2	1	10

U žádného nebezpečí v tomto subprocesu nedosáhla úroveň kritičnosti hodnoty 5. Všechna navrhovaná opatření jsou uvedena v přílohách.

Tabulka č. 21 – Akceptační testy

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Nedostatečná příprava jednotlivých testovacích prostředí	Chyba testera	Nekompatibilnost funkčností systémů	2	4	1	8
Závažné chyby v některých systémech	Chyba systému	Nekompatibilnost funkčností systémů	1	4	2	8
Opomenutí otestování některého z kritických systémů, bez kterého nelze pokračovat v testech	Chyba vedoucího regresních testů	Zablokování testů, nefunkčnost systému	1	**5**	1	5

Nebezpečí, které je pro tento subproces kritické, je opomenutí otestovat některý z kritických systémů, bez kterého nelze pokračovat v testech. Může se jednat například o testování přístupu do internetového bankovnictví klienta, přístup do klíčových databází apod.

Bez těchto přístupů nemůže uživatel klienta odbavit, protože nezíská klíčové informace, proto je důležité tyto systémy otestovat.

Navrhované řešení je provést testování kritických systémů opakovaně a nastavit prioritu jednotlivých systémů tak, aby nedošlo k opomenutí některého z nich.

Tabulka č. 22 – Testy funkčních požadavků

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Chyby v nových funkčnostech, na kterých se ještě pracuje	Chyba vývojáře, nedostatek času pro kontrolu	Nefunkčnost systémů, metodiky a funkčností	3	3	1	9
Chyby v regresních funkčnostech (staré funkčnonsti)	Chyba vývojáře	Nefunkčnost systémů, metodiky a funkčností	2	3	1	6

U žádného nebezpečí v tomto subprocesu nedosáhla úroveň kritičnosti hodnoty 5. Všechna navrhovaná opatření jsou uvedena v přílohách.

Tabulka č. 23 – Testy nefunkčních požadavků

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Neodstranění všech významných zranitelností systému při penetračních testech	Chyba vývojáře, testera	Zneužití zranitelností	5	**5**	5	125
Omezující technické podmínky pro provedení zátěžových testů (vyřazení určité transakce z testů)	Obtížná příprava potřebných testovacích dat, nedostatek prostředků pro vytvoření adekvátního testovacího prostředí	Některé business transakce nebudou dostatečně otestovány, v produkčním prostředí může dojít k přetížení	2	4	1	8
Při realizaci zátěžových testů není generována dostatečná zátěž významných business transakcí	Výkonnostní akceptace řešení nebere v úvahu další faktory, jako změna technologie, upgrade na novou verzi, nebo významnou změnu konfigurace	Pomalá odezva IS nebo nedostupnost požadovaných informací v provozní špičce	3	**5**	3	45
Nedostatečné zabezpečení polí editovatelných uživatelem	Chyba vývojáře, testera	Zneužití nebo ztráta dat skrze SQL injection, poškození dobrého jména podniku	2	**5**	4	40

Testy nefunkčních požadavků jsou klíčové v oblasti zabezpečení a zajištění spolehlivosti a dostupnosti informačního systému. V případě, že nejsou odstraněny všechny zranitelnosti při penetračních testech, může tuto zranitelnost objevit někdo jiný, kdo ji využije

(zero-day attack). Pravděpodobnost, že vývojáři a testeři neodstraní všechny zranitelnosti, je vysoká, protože je nemožné odstranit všechny zranitelnosti a tento stav dlouhodobě udržet.

Opatření proti tomuto riziku může být používání nejen automatizovaných, ale zejména i manuálních nástrojů pro provádění penetračních testů. Testy mohou provádět interní testeři a vývojáři, ale i externí testeři, kteří uzavřeli s bankou smlouvu o mlčenlivosti.

Dalším nebezpečím je generování nedostatečné zátěže významných business transakcí při realizaci zátěžových testů. Je to dáno tím, že kritéria úspěšnosti těchto testů nemusí brát v úvahu další faktory, jak je změna technologie, upgrade na novou verzi, nebo významnou změnu konfigurace. Následkem je pak přetížení informačního systému, pomalá reakce na požadavek uživatele a v nejhorším případě nedostupnost v provozní špičce.

Jako opatření může sloužit provádění analýzy testovaného systému a stanovení rozsahu zátěžových testů. Tento rozsah by měl zahrnovat zjištění limitů HW a SW konfigurace, optimalizaci této konfigurace a ověření výkonnosti po změně technologie, po upgradu a po významné změně konfigurace.

Dalším kritickým nebezpečím je nedostatečné zabezpečení polí editovatelných uživatelem. Tím jsou myšlena všechna pole, kam může uživatel informačního systsému vepisovat písmena, čísla a znaky. Vývojáři a testeři zajišťují znakové omezení do těchto polí pro případ, že by některý uživatel použil SQL injection, a tím získal interní data.

Opatřením může být nejen znakové omezení, například zvláštních znaků, ale také použití tříd a funkcí, které umožňují oddělit SQL dotaz od vstupních proměnných a zakázat relevantní SQL příkazy, zejména příkazy DELETE, DROP, ALTER a TRUNCATE.

2.9.7 Nasazení nového informačního systému

Proces nasazení nového informačního systému se skládá ze čtyř subprocesů. Identifikovaná nebezpečí jsou uvedena v tabulkách č. 24, 25, 26 a 27..

Tabulka č. 24 - Příprava

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Neodhadnutí termínu nasazení	Prodloužení doby interního vývoje, dodatečné požadavky na IS, nedostatek času pro správné otestování, chyby v kódech	Prodloužení doby nasazení IS, prodražení projektu	5	4	5	100
Nedostatek koncových uživatelů, kteří by testovali chyby v pilotním režimu	Pracovníci jsou příliš vytížení svou prací, pilotní režim testují v přesčasových hodinách apod.	Prodloužení doby pilotního režimu	2	3	1	6
Nedostatečné proškolení uživatelů	Nepřipravenost team leadrů a školitele, nekvalitně zpracovaná dokumentace k IS	Uživatel není schopen v IS pracovat, prodlužuje se doba odbavení klienta, zvýšené hlášení chybových požadavků na helpdesk	3	4	4	48

U žádného nebezpečí v tomto subprocesu nedosáhla úroveň kritičnosti hodnoty 5. Všechna navrhovaná opatření jsou uvedena v přílohách.

Tabulka č. 25 – Definování krizových scénářů

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Neodhadnutí nebo chybné nastavení minimální konfigurace	Chyba helpdesku	Zpomalení zpracování procesů a systémů,	1	4	1	4
Nedostatečné testování v pilotním režimu	Zadavatel chce urychlit proces nasazení IS	Chyby v ostrém provozu, nezajištění plynulého provozu	1	**5**	1	5
Nedefinování všech krizových scénářů	Opomenutí některého krizového scénáře projektovým týmem nebo přijetí rizika	Scénář nemusí nastat, a pokud ano, dojde k roll-backu	1	**5**	1	5

Kritická nebezpečí v tomto subrocesu jsou dvě. Krizový scénář popisuje celý harmonogram a postup nasazení informačního systému. Nedodržení tohoto postupu většinou znamená roll-back systému, tedy nejhorší možný výsledek nasazení. Nedostatečné testování v pilotním režimu je způsobeno většinou tlakem ze strany zadavatele na urychlení procesu nasazení. Prodloužení kterékoliv fáze znamená zvýšení ceny celého projektu. Pilotní testování přímo snižuje dopad chyb v provozu, které způsobí jeho neplynulý chod. Pro pilotní testování by měla být vymezena dostatečná časová rezerva. Jedině tak se zajistí plynulý provoz v produkčním prostředí.

Nedefinování všech krizových scénářů je nebezpečí, kterému se nelze vyhnout. Nedefinování všech scénářů znamená, že projektový tým některé nebezpečí opomenul, nebo jej přijmul a rozhodl se, že toto riziko podstoupí, a proto scénář nedefinoval. Pokud by k takovému scénáři došlo, v závislosti na závažnosti dojde k roll-backu, a termín nasazení se posunuje na pozdější. Zároveň dochází k prodražení celého projektu. Tomuto nebezpečí se dá do určité míry zamezit pouze tak, že krizové scénáře zhotoví více expertů nezávisle na sobě a tyto scénáře další experti zkontrolují. Požadovaný výsledek je stanovit všechny krizové scénáře, ke kterým může při nasazování informačního systému dojít.

Tabulka č. 26 - Odstávka

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Nedodržení harmonogramu odstávky	Technické problémy v migraci, chyba týmu	Roll-back systému	2	**5**	1	10
Nedodržení postupu nasazení	Chyba realase managera	Prodloužení odstávky, klienti nemají přístup na své účty, roll-back systému	1	**5**	1	5
Neodhalení chyb ve smoke testu	Chyba testera nebo kohokoliv z projekčního týmu	Nedodržení harmonogramu odstávky	1	4	1	4
Nezálohování původního stavu systému	Chyba nasazovacího týmu	Ztráta funkční konfigurace IS, úplná ztráta dat, ztráta posledních nových funkčností, dostupná pouze nefunkční verze	1	**5**	3	15

V tomto subprocesu jsou identifikována tři nebezpeční jako kritická. Postup odstávky se řídí podle určitého časového harmonogramu tak, aby klienti byly co nejméně omezeni ve využívání bankovních služeb. Nedodržením tohoto harmonogramu dojde k roll-backu systému a nasazení se přesouvá na jiný termín. Toto nedodržení můžou způsobit technické problémy v migraci, nebo je může způsobit některý člen z nasazovacího týmu.

Jako opatření slouží přesný popis harmonogramu, který musí být dodržen. Pro kritické části by měla být vymezena dostatečná časová rezerva, aby se předešlo zbytečnému roll-backu. Nasazovací tým by měl být složen z dostatečného počtu zkušených expertů, kteří se vyhnou jakékoliv chybovosti, zajistí dostatečné otestování před nasazením, nasadí správnou verzi IS a zajistí zálohování veškerých dat.

Dalším kritickým nebezpečím je nedodržení postupu nasazení IS. Za dodržení postupu nasazení zodpovídá realase manager. Chyby se může dopustit kdokoliv z nasazovacího týmu,

nebo se může jednat o chybu v systému. Výsledkem je prodloužení doby odstávky, nebo roll-back systému.

Jak již bylo zmíněno, za nasazení zodpovídá realase manager, který kontroluje splnění jednotlivých kroků v harmonogramu. Každý člen expertního týmu po sobě kontroluje část, za kterou je odpovědný. Vzhledem k tomu, že dodržení postupu je pouze záležitostí dostatečné kontroly, nebyla navržena žádná další opatření.

Dalším, velmi kritickým nebezpečím, je nezálohování původního stavu systému. Pravděpodobnost tohoto nebezpečí je velmi nízká, ale dopad je katastrofální. V případě nezálohování původního stavu systému dojde ke ztrátě funkční konfigurace informačního systému, ztrátě posledních nových funkčností a k částečné nebo úplné ztrátě dat. Banka bude mít k dispozici pouze nefunkční verzi informačního systému.

Současné opatření je vícečetná kontrola zálohování původního stavu systému. Tuto kontrolu by měl také provádět realase manager, který je za celé nasazení zodpovědný.

Tabulka č. 27 - Provoz

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Uživatelé nejsou schopni pracovat v novém IS	Nasazení špatné verze IS, která je nekompatibilní se systémy, které byly nasazeny s danou verzí IS, chyba dodavatele balíků (nasazovací tým)	Uživatel nemůže odbavit klienta po telefonu ani provádět aktivní operace na účtu	2	**5**	1	10
Výpadek některých systémů, které jsou kritické pro funkčnost IS	Přetížení systému, odstávka elektřiny, zhroucení některého systému	Neplynulý provoz, pomalejší, nebo žádné odbavení klienta	1	**5**	1	5

V tomto subprocesu byla všechna identifikovaná nebezpečí hodnocena jako kritická. Ve chvíli, kdy je spuštěn nový informační systém a uživatelé nejsou schopni v systému pracovat, dojde ke kritickému okamžiku, kdy banka není schopna odbavit klienty po telefonu a provádět aktivní operace. K tomuto stavu dojde, pokud je nasazena špatná verze informačního systému, která je nekompatibilní s ostatními systémy, které byly nasazeny s danou verzí informačního systému.

Této situaci lze předcházet kontrolou dodávaných balíků a verzí, a kontrolou nasazované verze realase managerem, který zodpovídá za celý proces nasazení informačního systému.

Další nebezpečí spočívá ve výpadku některých systémů, které jsou kritické pro funkčnost. Může se jednat například o propojení informačního systému s internetovým bankovnictvím klienta. Pokud by došlo k tomuto výpadku a zároveň klient požadoval provést neodkladný převod peněz na jiný účet, uživatel by tento převod nedokázal provést, a musel by klienta odkázat na pobočku, mobilní aplikaci nebo na internetové bankovnictví.

Jak postupovat v případě výpadku některého z kritických systémů popisuje krizový plán. Banka musí mít zajištěné záložní pracoviště, odkud může uživatel odbavit klienta. Tyto krizové plány by také měly být popsány v dokumentaci pro potřeby projektového týmu, a zejména ostatních uživatelů informačního systému.

2.9.8 Odstranění chyb

Proces odstranění chyb nezahrnuje žádné další subprocesy. Identifikovaná nebezpečí jsou uvedena v tabulce č. 28.

Tabulka č. 28 – Odstranění chyb

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Neodstraní se všechny chyby	Chyba vývojářů nebo tlak na urychlení procesu nasazení	Nefunkčnost některých systémů	3	4	1	12
Odstraněná chyba způsobí další chybu	Vývojář neopraví všechny chyby, které se vyskytnou po změně kódu, nebo systémová analýza obsahuje nedostatky	Neplynulý provoz, ztížení některých procesů, nedostatečná funkčnost	2	4	1	8
Chybám se neuděluje priorita (nebo nerelavantní priorita)	Uživatel si neuvědomuje rozsah chyb	Odstraňování chyb ve špatném pořadí	4	4	2	32

U žádného nebezpečí v tomto subprocesu nedosáhla úroveň kritičnosti hodnoty 5. Všechna navrhovaná opatření jsou uvedena v přílohách.

2.9.9 Akceptace projektu

Proces akceptace projektu se skládá pouze z jednoho subprocesu. Identifikovaná nebezpečí jsou uvedena v tabulce č. 29.

Tabulka č. 29 – Akceptace projektu

Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	O	S	D	RPN
Dokumentace k IS je nepřehledná nebo neúplná	Zadavatel nedostatečně specifikuje požadavky na dokumentaci, nebo zhotovitel opomene některé z těchto požadavků	Prodloužení doby při řešení problémů popsaných v dokumentaci, nutnost další komunikace s dodavatelem	3	**5**	1	15
Zhotovitel neposkytuje dostatečnou technickou podporu pracovníkům projektu zadavatele	Smlouva neobsahuje všechny náležitosti, zejména dodatek o technické a uživatelské podpoře, nebo zhotovitel nedodržuje smluvní podmínky	Bez technické podpory zhotovitele IS je vytváření nových funkčností složité a zdlouhavé	2	**5**	1	10
Zhotovitel nedodá všechny požadované protokoly pro funkčnost IS zadavateli, nebo jsou tyto protokoly neúplné	Chyba na straně zhotovitele	Chyby ve funkčnostech IS	2	**5**	1	10
Zadavatel má k projektu výhrady a projekt nechce akceptovat	IS neodpovídá představám zadavatele, příčina může být ve kterékoliv části procesu	Pokud zhotovitel vytvořil a implementoval IS podle požadavků zadavatele a podle Service Level Agreement, zadavatel projekt musí akceptovat a doplatit zbývající částku za projekt	4	**5**	1	20

Všechna nebezpečí, která byla v tomto procesu identifikována, mohou být pro celý projekt kritická. V případě, že zhotovitel nedodá k informačnímu systému přehlednou, použitelnou a úplnou dokumentaci, dojde k prodloužení doby řešení jednotlivých chyb, které měly být detailně a přehledně popsány v dokumentaci. Dokumentace také popisuje práci v jednotlivých složkách informačního systému a má sloužit jako podklad uživatelům pro práci v informačním systému. Jestliže uživatelé v dokumentaci nenajdou postupy, které potřebují, prodlužuje se tak doba řešení a zpracovávání jednotlivých úkolů.

Řešením této situace může být vícečetná kontrola dokumentace nejen projektovým týmem, ale zejména vybranými uživateli, kteří s dokumentací a informačním systémem denně pracují. Uživatelé identifikují slabá místa v dokumentaci a zhotovitel tato slabá místa doplní.

Dalším kritickým nebezpečím je neposkytování dostatečné technické podpory zhotovitelem informačního systému. Po předání a akceptaci projektu práce zhotovitele nekončí. Zavazuje se, že bude podniku dodávat aktuální verze, uvolňovat patche, poskytovat technickou podporu a další služby. Všechny tyto informace by měly být uvedeny ve smlouvě.

Pokud je zhotovitel nedodržuje, může tím způsobit podniku významné potíže. Interní vývojáři podniku mohou mít problémy zejména s rozšiřitelností systému, přidáváním nových funkčností apod.

Ošetřením rizika může být zpracování požadavků na informační systém podle metodiky ITIL, případně smlouvu doplnit o Operational Level Agreement. Důležité je také stanovit způsob sankciování zhotovitele za nedodržení jednotlivých bodů smlouvy.

Dalším nebezpečím je nedodání všech požadovaných protokolů pro funkčnosti informačního systému zadavateli, nebo dodání neúplných protokolů. Opět se jedná o nedodržení podmínek zhotovitelem. Výsledkem mohou být chyby v jednotlivých funkčnostech. Tomuto nebezpečí se dá předejít pouze výběrem vhodného zhotovitele například podle referencí, osobní zkušenosti apod. Zhotovitel by měl požadované protokoly dodat nejen všechny a úplné, ale také včas.

Pokud zhotovitel navrhne a implementuje informační systém podle požadavků, ale výsledek neodpovídá představě zadavatele, zadavateli nezbývá nic jiného, než projekt akceptovat a zaplatit. Příčina může být ve kterékoliv části procesu. Nejčastější příčina bývá nevyjasnění si jednotlivých požadavků, návrh uživatelského prostředí, opomenutí funkčních a nefunkčních požadavků apod. Je tedy klíčové, aby zhotovitel vracel všechny nepřesně definované požadavky zpět zadavateli, a aby zadavatel zajistil dostatečný počet pracovníků podniku, kteří se budou věnovat výběru a implementaci nového informačního systému.

Opatřením proti tomuto nebezpečí je zajištění dostatečné časové rezervy pro klíčové fáze projektu, zejména pro fáze stanovení požadavků a vytváření návrhu. Dalším opatřením může být zmíněné zapojení koncových uživatelů na stanovování těchto požadavků, účast na pilotním režimu apod.

ZÁVĚR

Hlavním cílem této diplomové práce bylo provedení procesní analýzy FMECA na zavedení nového informačního systému v bance. Měla být stanovena taková opatření, která povedou ke snížení dopadu nebezpečí, nebo ke snížení pravděpodobnosti jejich výskytu.

Pro splnění hlavního cíle byla v každém procesu identifikována nebezpečí, stanovena pravděpodobnost jejich výskytu, jejich závažnost a pravděpodobnost včasné detekce. Dále bylo vypočteno prioritně rizikové číslo, které určuje celkovou závažnost tohoto nebezpečí. Pro jednotlivá nebezpečí byla stanovena opatření, které vedla ke snížení prioritně rizikového čísla. Největší pozornost byla věnována těm nebezpečím, jejichž hodnota závažnosti byla pro proces velmi závažná až kritická. Pokud by tato nebezpečí nebyla ošetřena, došlo by k finanční ztrátě, ke ztrátě dat, poškození dobrého jména, nebo k ukončení podnikatelské činnosti. Těchto nebezpečí bylo 28 z celkového počtu 63 identifikovaných nebezpečí.

Pro splnění dílčího cíle byla provedena analýza vnitřního a vnějšího prostředí ve vztahu k informačnímu systému. Z těchto analýz byla vytvořena SWOT matice, jejíž výstupem bylo doporučení zavést takový informační systém, který bude sloužit uživatelům jako jednotné pracovní místo, povede k nákladové optimalizaci a zrychlí některé procesy v podniku.

Tato diplomová práce může sloužit bance jako podklad pro proces zavedení nového informačního systému, který by mohl být v budoucnu zrealizován. Cíl práce byl tedy splněn a uskutečnění projektu je reálné.

SEZNAM POUŽITÝCH LITERÁRNÍCH ZDROJŮ

[1] ČERMÁK, M. *Řízení informačních rizik v praxi.* 1. vyd. Brno: TRIBUN EU, 2009. 134 str. ISBN 978-80-7399-731-1.

[2] JANÍČEK, P. a kol. *Expertní inženýrství v systémovém pojetí.* 1. vyd. Praha: GRADA PUBLISHING, a.s., 2013. 592 str. ISBN 978-80-7204-554-9.

[3] PROCHÁZKOVÁ, D. *Metody, nástroje a techniky pro rizikové inženýrství.* 1. vyd. Praha: NAKLADATELSTVÍ KAROLINUM, 2011. 369 str. ISBN 978-80-01-04842-9.

[4] RAIS, K. DOSKOČIL, R. *Risk management.* 1. vyd. Brno: AKADEMICKÉ NAKLADATELSTVÍ CERM, s.r.o. Brno, 2007. 152 str. ISBN 978-80-214-3510-0.

[5] RAIS, K. DOSKOČIL, R. *Operační a systémová analýza I.* Brno: VUT v Brně, Fakulta podnikatelská, 2006, 107 s., ISBN 80-214-3280-2.

[6] SMEJKAL, V. RAIS, K. *Řízení rizik ve firmách a jiných organizacích. 4. dopl. Vyd.* Praha: GRADA PUBLISHING, s.r.o., 2013. 488 str. ISBN 978-80-247-4644-9.

[7] TICHÝ, M. *Ovládání rizika. Analýza a management.* 1. vyd. Praha: BECKOVA EDICE EKONOMIE, 2006. 396 str. ISBN 80-7179415-5.

SEZNAM POUŽITÝCH NOREM

[8] ČSN EN 608 12 (01 0675). *Techniky analýzy bezporuchovosti systémů – Postupy analýzy způsobů a důsledků poruch (FMEA).* Praha: Český normalizační institut, 2007.

[9] ČSN ISO 31000 (001 0351). *Management rizik - Principy a směrnice.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010.

[10] ISO/IEC 27005 (36 9790). *Řízení rizik bezpečnosti informací.* Praha: Český normalizační institut, 2009.

SEZNAM POUŽITÝCH ELEKTRONICKÝCH ZDROJŮ

[11] Analýza pěti sil 5F. *Management mania* [online] 2016. [cit 2017-02-01]. Dostupné z: https://managementmania.com/cs/analyza-5f

[12] Analýza rizik: Jemný úvod do analýzy rizik. *Clever and Smart* [online] 2010. [cit 2017-02-01]. Dostupné z: http://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/

[13] Avoiding Commong FMECA Mistakes. *FMEA - FMECA* [online] 2006. [cit 2017-02-01]. Dostupné z: http://www.fmea-fmeca.com/common-fmea-mistakes.html

[14] Identifikace a popis rizik. *Brain Tools Club* [online] 2015. [cit 2017-02-01]. Dostupné z: http://www.braintools.cz/toolbox/zvladani-rizik/identifikace-a-popis-rizik.htm

[15] Konsolidovaná výroční zpráva Air Bank, a.s. za rok 2016. *Air Bank* [online] 2017. [cit 2017-02-01]. Dostupné z: https://www.airbank.cz/file-download/vyrocni-zprava-2016.pdf

[16] Konsolidovaná výroční zpráva 2015. *Equa Bank* [online] 2016. [cit 2017-02-01]. Dostupné z: https://www.equabank.cz/download/archiv/22008809033028/838-vz-equabank-2015-cz.pdf

[17] Mobilní bankovnictví. Kolik klientů používá smartbanking? *Finparada* [online] 2015. [cit 2017-02-01]. Dostupné z: http://www.finparada.cz/3104-Mobilni-bankovnictvi-posledni-dil-serialu-na-Finparade.aspx

[18] Porovnání bank. *Geen Vstřícná banka* [online] 2017. [cit 2017-02-01]. Dostupné z: https://www.vstricnabanka.cz/porovnani-bank/2016/

[19] Typy organizačních struktur a jejich členění. *Business Info CZ* [online] 2010. [cit 2017-02-01]. Dostupné z: http://www.businessinfo.cz/cs/clanky/typy-organizacnich-struktur-cleneni-2840.html#!&chapter=4

[20] Výběr informačního systému. *Systém online* [online] 2001. [cit 2017-02-01]. Dostupné z: https://www.systemonline.cz/clanky/vyber-informacniho-systemu.htm

[21] Výdaje na výzkum a vývoj poprvé překročily 80 miliard. *Český statistický úřad* [online] 2015. [cit 2017-02-01]. Dostupné z: https://www.czso.cz/csu/czso/vydaje-na-vyzkum-a-vyvoj-poprve-prekrocily-80-miliard

[22] Výroční zpráva Fio Bank. *Fio Bank* [online] 2016. [cit 2017-02-01]. Dostupné z: https://www.fio.cz/docs/cz/Fio_banka_VZ_2015_CZ.pdf

[23] Výroční zpráva končící k 31.12.2015. *Commerz Bank* [online] 2016. [cit 2017-02-01]. Dostupné z: https://www.commerzbank.cz/portal/media/corporatebanking/auslandsseiten/tschechien-informationen/englisch-tschechisch/impressum-4/Vron_zprva_2015_COBA_Praha__FINAL.pdf

[24] Výroční zpráva 2015. *ČSOB* [online] 2016. [cit 2017-02-01]. Dostupné z: http://www.csas.cz/static_internet/cs/html/csvz/index.html

[25] Výroční zpráva 2015. *Komerční banka* [online] 2016. [cit 2017-02-01]. Dostupné z: https://www.kb.cz/file/cs/o-bance/vztahy-s-investory/publikace/vyrocni-zpravy/kb-2015-vyrocni-zprava.pdf?2079ac9a8c9b93989d387f79c46dd7f

[26] Výroční zpráva 2015. *Raiffeisenbank CZ* [online] 2016. [cit 2017-02-01]. Dostupné z: https://www.rb.cz/attachments/vyrocni%20zpravy/vz-rb-15-cz.pdf

[27] Vývoj pojistného trhu. *Česká asociace pojišťoven* [online] 2016. [cit 2017-02-01]. Dostupné z: http://www.cap.cz/statisticke-udaje/vyvoj-pojistneho-trhu

[28] Základní informace. *Česká spořitelna* [online] 2016. [cit 2017-02-01]. Dostupné z: http://www.csas.cz/static_internet/cs/Obecne_informace/FSCS/CS/Prilohy/cs_vz2015.pdf

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

Příloha č. 1 – FMECA: Stanovení požadavků na IS

Proces	Subproces	Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	Současná opatření	O	S	D	RPN	Fáze odhalení	Doporučená opatření	O	S	D	RPN
STANOVENÍ POŽADAVKŮ NA IS	Stanovení požadavků managementu	Nedostatečný budget na zhotovení IS	Neočekávané investice do jiných projektů, strategické rozhodnutí	Nenalezení zhotovitele IS, který by přijal finanční nabídku, nebo oslovení nevhodných zhotovitelů	Přealokování peněz v rámci banky a/nebo výběr levnějšího IS	2	5	1	10	Výběrové řízení	Žádost o úvěr, nalezení vhodného investora	1	5	1	5
		Nereálné očekávané přínosy	Přeceňování technických prostředků bez zajištění přiměřených odpovídajících procesů, přeceňování návratnosti investice, která není vždy vyčíslitelná	Negativní postoj k dalším investicím do ICT nebo naopak další přemrštěné investice	Zajištění evidence vykazování přínosů, znalost současného stavu nákladových položek pro objektivní porovnání, objektivní měření úspor	4	4	4	64	Výběrové řízení	Konkretizace a měřitelnost očekávaných přínosů, zahrnutí nevyčíslitelných přínosů do evidence vykazování přínosů, řízení nákladů a přínosů, které souvisí s návrhem, realizací a provozováním IS	2	4	2	16
		Stanovení krátkého časového limitu na projekt	Nereálný odhad doby trvání projektu, nedostatečná příprava podkladů a spolupráce projektového týmu s ostatními pracovníky podniku	Zvýšení nákladů na IS, odmítnutí projektu dodavatelem, prodloužení doby interního vývoje	Stanovení orientačního termínu zavedení nového IS	5	4	5	100	Ve kterékoliv fázi	Použití metody kritické cesty s časovou rezervou v projektu, konzultace s pracovníky podniku, zejména s vývojáři, testery a softwarovými architekty	3	4	5	60
	Stanovení technických požadavků	Opomenutí některého z technických požadavků na IS	Chyba vedoucího IT infrastructure	Zvýšení nákladů na provoz na technické vybavení, dodatečné změnové požadavky na IS	Technické požadavky jsou stanoveny podle soupisu technického vybavení podniku	1	4	5	20	Implementace	Pravidelná aktualizace soupisu technického vybavení	1	4	1	4
		Chybná specifikace technických požadavků	Chyba vedoucího IT infrastructure	Zvýšení nákladů na provoz na technické vybavení, dodatečné změnové požadavky na IS	Technické požadavky jsou stanoveny podle soupisu technického vybavení podniku	1	4	5	20	Implementace	Pravidelná aktualizace soupisu technického vybavení	1	4	1	4
	Stanovení nefunkčních požadavků	Opomenutí některého nefunkčního požadavku	Chyba vedoucího IT security	IS postrádá důležité vlastnosti, zvýšení nákladů, prodloužení doby interního vývoje, IS nepředstavuje konkurenční výhodu a návratnost investice neodpovídá očekávané	Stanovení nefunkčních požadavků podle interní metodiky	2	5	5	50	Ve kterékoliv fázi	Stanovení nefunkčních požadavků v Service Level Agreement podle metodiky ITIL	1	5	2	10
		Nepřesná specifikace jednotlivých požadavků	Chyba vedoucího IT security	IS postrádá důležité vlastnosti, zvýšení nákladů, prodloužení doby interního vývoje, IS nepředstavuje konkurenční výhodu a návratnost investice neodpovídá očekávané	Stanovení nefunkčních požadavků podle interní metodiky	2	5	5	50	Ve kterékoliv fázi	Stanovení nefunkčních požadavků v Service Level Agreement podle metodiky ITIL	1	5	2	10

Příloha č. 2 – FMECA: Výběrové řízení

Proces	Subproces	Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	Současná opatření	O	S	D	RPN	Fáze odhalení	Doporučené opatření	O	S	D	RPN
VÝBĚROVÉ ŘÍZENÍ	Oslovení zhotovitelů IS	Nezájem zhotovitelů o zakázku	Nedostatek času a/nebo kapacity oslovených zhotovitelů	Prodloužení doby výběrového řízení z důvodu nedostatku zájemců o projekt	Oslovení dalších zhotovitelů, včetně zhotovitelů ze zahraničí	4	5	1	20	Výběrové řízení	Výběr zhotovitele, který je schopen splnit požadavky na IS a odložení projektu do doby, než bude mít vybraný zhotovitel na projekt čas a kapacitu	3	5	1	15
		Oslovení nesprávných zhotovitelů	Nedostatek zhotovitelů IS na trhu, zadavatel nemá dostatek informací o všech potenciálních zhotovitelích	Nevyhovující návrh od potenciálního zhotovitele	Hledání jiného vhodného zhotovitele IS	4	4	1	16	Výběrové řízení	Účast kompetentních pracovníků banky na výběrovém řízení, vyřazení nabídek, které nespecifikují řešení významných a specifických požadavků IS	3	4	1	12
	Výběrové řízení	Nepřihlásí se žádný zhotovitel	Oslovení zhotovitelé nedokážou vyhovět požadavkům na IS nebo je pro ně nabídka finančně nezajímavá	Prodloužení doby výběrového řízení z důvodu nedostatku zájemců o projekt	Úprava požadavků na IS, oslovení dalších potenciálních zhotovitelů včetně zahraničních	3	5	1	15	Výběrové řízení	Navýšení budgetu úvěrem nebo investorem, přehodnocení těch požadavků, které nejsou oslovení zhotovitelé schopni splnit	2	4	1	8
		Zmanipulování výběrového řízení	Korupce	Výběr nevhodného zhotovitele, nový IS nepřispívá k získání konkurenční výhody a/nebo růstu tržeb a dalších očekávaných přínosů	Hromadné schválení zhotovitele informačního systému odpovědnými osobami	2	5	5	50	Nikdy nebo ve kterékoliv fázi	Hlasy jednotlivců skupiny, která vybírá zhotovitele IS, mají stejnou váhu a musí souhlasit více než 60% hlasujících	1	5	5	25
		Výběr špatného zhotovitele	Nedostatečný budget na zhotovení informačního systému a/nebo nevyjasnění si specifických požadavků na IS se zhotovitelem	Zvýšení nákladů na další rozvoj IS, projekt nevede k očekávané ekonomické efektivnosti	Účast kompetentních pracovníků banky na výběrovém řízení, více kol výběrového řízení	4	5	5	100	Ve kterékoliv fázi	Ověření referencí u jiných firem, které využívají informační systém vybraného zhotovitele	3	5	5	75
		Licenční omezení	V nabídce zhotovitele jsou uvedeny podmínky pro zakoupení dalších licencí, které nejsou započteny do konečné ceny projektu	Překročení budgetu	Vyjednávání o ceně licence	4	4	5	80	Výběrové řízení / Akceptace	Výběr takového zhotovitele, který je ochoten snížit cenu dodatečných licencí	2	4	2	16

Příloha č. 3 – FMECA: Vytváření specifikací

Proces	Subproces	Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	Současná opatření	O	S	D	RPN	Fáze odhalení	Doporučené opatření	O	S	D	RPN
VYTVÁŘENÍ SPECIFIKACÍ NA IS	Business specifikace	Nepřesnosti v popisu jednotlivých procesů	Nepoužívání business slovníku	Řešitel business požadavků nemusí všechny požadavky pochopit správně	Nejsou stanoveny	5	3	1	15	V každé fázi	Sepsání business slovníku s preciznou definicí pojmů	2	3	1	6
		Opomenutí části procesu	Chyba business analytika	Zvýšené provozní náklady, prodloužení doby projektu	Kontrola popisu procesů odpovědnou osobou	2	3	4	24	Návrh / Testování	Stanovení metodických pravidel pro stanovování business specifikace, vytvoření procesní mapy už ve fází popisu business specifikace	1	3	1	3
		Zjednodušení procesu	Business analytik nedefinuje proces detailně	Prodloužení doby návrhu	Kontrola popisu procesů odpovědnou osobou	3	3	4	36	Návrh / Testování	Stanovení metodických pravidel pro stanovování business specifikace, vytvoření procesní mapy už ve fází popisu business specifikace	2	3	1	6
	Business analýza	Špatně popsaná procesní napa	Solution architekt nedefinuje proces detailně	Prodloužení doby návrhu, zhotovitel neporozumí zadání IS	Pravidelná kontrola práce solution architekta odpovědnou osobou	4	3	3	36	Testování	Častější schůzky se zhotovitelem a dalšími členy projektového týmu	2	3	1	6
		Vytváření zbytečných procesů navíc	Nedostatečné množství schůzek solution architekta se zadavatelem a zhotovitelem	Prodloužení doby návrhu, zvýšení nákladů na projekt	Pravidelné schůzky solution architekta s dalšími členy projektového týmu	2	3	3	18	Provoz	Kontrola procesní mapy více experty	1	3	1	3
	Systémová analýza	Opomenutí bezpečnostních opatření jednotlivých databází a systémů	Nedostatečné testování zabezpečení těchto databází a systémů	Prodloužení doby testování, zvýšené náklady, možnost napadení systémů	Správná metodika bezpečnostních testů, ověřování přes certifikáty, šifrovaná spojení	1	5	5	25	Testování	Na bezpečnostních opatřeních se podílí tým složený z bezpečnostních inženýrů a analytiků	1	5	3	15
		Chybné stanovení propojení IS s jednotlivými databázemi	Chyba solution architekta	IS neposkytne požadované informace uživateli	Spolupráce business analytika a solution architekta, detailní znalost interních systémů a databází	1	5	5	25	Implementace	Přístup oprávněným osobám do dokumentace kde je popsaná architektura systému, následná kontrola	1	5	2	10

Příloha č. 4 – FMECA: Vytváření návrhu

Proces	Subproces	Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	Současná opatření	O	S	D	RPN	Fáze odhalení	Doporučené opatření	O	S	D	RPN
VYTVÁŘENÍ NÁVRHU	Projekční část	Vytvoření nereálného časového plánu pro zavedení IS	Chyba projekt managementu	Prodražení a prodloužení očekávané doby zhotovení IS	V návrhové části se stanovuje pouze orientační datum nasazení IS	5	4	5	100	Ve kterékoliv části projektu	Stanovení časové rezervy v časovém harmonogramu	3	4	6	72
		Nevytvoření všech potřebných testovacích prostředí	Chyba test designera nebo test managera	Nemožnost otestování všech funkcí IS	Vytvoření potřebných testovacích prostředí v průběhu testování	5	2	5	50	Testování	Stejné jako současné	5	2	5	50
		Rozpočet nezahrnuje všechny nákladové položky IS	Zhotovitel zatají některé zpoplatněné služby které jsou součástí IS, např. přístupy, programové úpravy, hotline apod.	Výsledná cena je odlišná	Ověření, že nabízení cena zahrnuje opravdu všechny náklady na IS	4	4	5	80	Akceptace projektu	Vyžádání si od dodavatele podrobnou cenovou nabídku se všemi dodatky, případně vyjednávání o ceně	3	4	5	60
		Chyba v návrhu business procesů	Chyba business analytika	Prodloužení doby vytváření návrhu, chyby v testování	Kontrola procesní mapy ještě před vytvářením návrhu	2	4	5	40	Testování	Opakované konzultace v průběhu vytváření návrhu	1	4	4	16
		Analýza rizik je vytvořena později než v návrhové části projektu nebo vůbec	Expertní tým, který analýzu provádí, nemá čas na včasné provedení analýzy, projekční tým nepřikládá analýze rizik dostatečnou důležitost	Prodloužení a prodražení projektu, neúspěšné dokončení, nedostatečné zabezpečení IS, ztráta dat o klientech	Sestavení expertního týmu ještě před vytváření návrhu a poskytnutí dostatku času na zhotovení analýzy	4	5	1	20	Vytváření návrhu	Zajištění expertního týmu ještě před výběrovým řízením, průběžná kontrola a doplňování položek do analýzy rizik celým projekčním týmem, nebo oslovení společnosti, která se analýzami rizik zabývá	1	5	1	5
	Technická část	Chyby v datovém modelování	Chyba vývojáře	Při práci v systému se zobrazí chyba, nebo se nezobrazí data, nebo je systém úplně nefunkční	Vývojář by měl mít k dispozici návrh business analytika	2	5	1	10	Ve kterékoliv části projektu	Skládání systému z jednotlivých modulů tak, aby na sobě byly co nejvíce nezávislé, při výskytu chyby v jednom modulu ostatní moduly fungují korektně	1	5	1	5
		Uživatelské prostředí vznikne až na základě datového modelu	Chyba designer vývojáře	V uživatelském prostředí nebudou všechny informace, které uživatele potřebuje, nebo jich bude zbytečně moc a systém se zpomaluje	Uživatelské prosředí vznikne ještě před vytvořením datového modelu, prostředí navrhuje designer vývojář	2	2	1	4	Vytváření návrhu	Schválení uživatelského prostředí business analytikem a zadavatelem	1	2	1	2

Příloha č. 5 – FMECA: Implementace

Proces	Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	Současná opatření	O	S	D	RPN	Fáze odhalení	Doporučené opatření	O	S	D	RPN
IMPLEMENTACE	Opomenutí uživatelských požadavků na IS	Nedostatečná zainteresovanost pracovníků banky na procesu zavádění IS	Změna zadání, změna časového harmonogramu, prodražení projektu	Změnové požadavky po nasazení	3	5	3	45	Implementace / Akceptace	Zajištění dostatečného množství kompetentních pracovníků banky na stanovování požadavků na IS a celém procesu zavádění	2	5	3	30
	Naprogramované uživatelské řešení odpovídá odsouhlasené analýze, ale ne představě zadavatele IS	Nepotvrzování si jednotlivých částí požadavků se zhotovitelem, nedostatečná zainteresovanost pracovníků banky na projektu	Dodatečné požadavky funkčností nad rámec analýzy, změna časového harmonogramu, prodražení projektu	Nejsou stanovena	5	5	3	75	Implementace / Akceptace	Zajištění dostatečného množství kompetentních pracovníků banky na stanovování požadavků na IS	3	5	3	45
	Chyby v migraci dat	Neodsouhlasení architektonických struktur, špatné naprogramování převodového můstku, neočištění dat před převodem	Chyba vývojáře	Zabezpečení struktury zdrojových dat, zajištění očištění dat jak pro testovací, tak pro ostrý převod dat	2	4	1	8	Implementace	Testovací migrace dat, testování struktury dat v novém IS	1	4	1	4

Příloha č. 6 – FMECA: Testování 1. část

Proces	Subproces	Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	Současná opatření	O	S	D	RPN	Fáze odhalení	Doporučené opatření	O	S	D	RPN
TESTOVÁNÍ	Vytváření test cases	Nepopsání testovacího scénáře v úplném rozsahu	Nedostatek času, chyba testera	Špatně provedené regresní testy (následující kolo testů nemusí odpovídat požadovaným výsledkům)	Zpřístupnění systémové analýzy testerům, prodloužení času	4	1	1	4	Testování	Časová rezerva pro stanovení testovacích scénářů	2	1	1	2
		Business zadavatel mění požadavky na systémovou analýzu v průběhu testování	Časté změny v systémové analýze	Prodloužení doby testování	Nejsou stanoveny	5	4	2	40	Testování	Dokončení požadavků na systémovou analýzu před začátkem procesu testování	3	4	2	24
		Testovací scénáře neodpovídají požadavkům systémové analýzy	Chyba v komunikaci mezi testery a analytiky	Špatná funkčnost systému	Zajištění komunikace mezi testery a analytiky	5	1	1	5	Testování / Provoz	Jednoznačně stanovené požadavky pro testování v systémové analýze	3	1	1	3
		Špatné výsledky úspěšnosti testů	Chyba testera	Možné prodloužení doby testování, s těmito chybami se počítá	Výsledky testů jsou zaznamenávány v reportech a postupně aktualizovány	5	1	1	5	Testování	Stejné jako současné	5	1	1	5
		Nevytvoření všech možných test cases	Chyba testera	Nedostatečné otestování	Nejsou stanoveny	5	2	1	10	Testování	Výběr zkušeného testera, který testovací scénáře vytváří	3	2	1	6
	Akceptační testy	Nedostatečná příprava jednotlivých testovacích prostředí	Chyba testera	Nekompatibilnost funkčností systémů	Nejsou stanoveny	2	4	1	8	Testování	Za přípravu testovacích prostředí odpovídá vedoucí testerů	1	4	1	4
		Závažné chyby v některých systémech	Chyba systému	Nekompatibilnost funkčností systémů	Kontrola před nasazením od vývojářů	1	4	2	8	Testování	Utilní testy	1	4	1	4
		Opomenutí otestování některého z kritických systémů, bez kterého nelze pokračovat v testech	Chyba vedoucího regresních testů	Zablokování testů	Opakované testování	1	5	1	5	Testování	Nastavení priorit jednotlivých systémů	1	5	1	5
	Testy funkčnostích požadavků	Chyby v nových funkčnostech, na kterých se ještě pracuje	Chyba vývojáře, nedostatek času pro kontrolu	Nefunkčnost systémů, metodiky a funkčností	Nejsou stanoveny	3	3	1	9	Testování	Časová rezerva pro kontrolu programování vývojářem	1	3	1	3
		Chyby v regresních funkčnostech (staré funkčnonsti)	Chyba vývojáře	Nefunkčnost systémů, metodiky a funkčností	Nejsou stanoveny	2	3	1	6	Testování	Kontrola vedoucím regresních testů	2	3	1	6

Příloha č. 7 – FMECA: Testování 2. část

Proces	Subproces	Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	Současná opatření	O	S	D	RPN	Fáze odhalení	Doporučené opatření	O	S	D	RPN
TESTOVÁNÍ	Testy nefunkčních požadavků	Neodstranění všech významných zranitelností systému při penetračních testech	Chyba vývojáře, testera	Zneužití zranitelností	Nejsou stanoveny, nelze odstranit všechny zranitelnosti	5	5	5	125	Testování / Provoz	Provádění penetračních testů nejen s použití automatizovaných nástrojů, ale i manuálně, testování interními testery i externí společností	4	5	4	80
		Omezující technické podmínky pro provedení zátěžových testů (vyřazení určité transakce z testů)	Obtížná příprava potřebných testovacích dat, nedostatek prostředků pro vytvoření adekvátního testovacího prostředí	Některé business transakce nebudou dostatečně otestovány, v produkčním prostředí může dojít k přetížení	Nejsou stanoveny	2	4	1	8	Testování	Výběr kritických business transakcí, které musí být otestovány, a pro ty vytvořit testovací prostředí a specifikovat testovací data, prodloužit harmonogram testování	1	4	1	4
		Při realizaci zátěžových testů není generována dostatečná zátěž významných business transakcí	Výkonnostní akceptace řešení nebere v úvahu další faktory, jako změna technologie, upgrade na novou verzi, nebo významnou změnu konfigurace	Pomalá odezva IS nebo nedostupnost požadovaných informací v provozní špičce	Provedení analýzy testovaného systému	3	5	3	45	Testování / Provoz	Rozsah zátěžových testů by měl zahrnovat zjištění limitů HW a SW konfigurace, optimalizaci HW a SW konfigurace a ověření výkonnosti po změně technologie, po upgradu a po významné změně konfigurace	2	5	2	20
		Nedostatečné zabezpečení polí editovatelných uživatelem	Chyba vývojáře, testera	Zneužití nebo ztráta dat skrze SQL injection, poškození dobrého jména podniku	Znakové omezení editovatelných polí, použití prepared statements	2	5	4	40	Testování / Provoz	Použití třídy nebo funkce, která umožňuje oddělit SQL dotaz od vstupních proměnných, zakázat relevantní SQL příkazy, jako jsou DELETE, DROP, ALTER, TRUNCATE	1	5	2	10

Příloha č. 8 – FMECA: Nasazení informačního systému

Proces	Subproces	Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	Současná opatření	O	S	D	RPN	Fáze odhalení	Doporučené opatření	O	S	D	RPN
NASAZENÍ INFORMAČNÍHO SYSTÉMU	Příprava	Neodhadnutí termínu nasazení	Prodloužení doby interního vývoje, dodatečné požadavky na IS, nedostatek času pro správné otestování, chyby v kódech	Prodloužení doby nasazení IS, prodražení projektu	Stanovení časové rezervy v harmonogramu	5	4	5	100	A	Stejná jako současná	5	4	5	100
		Nedostatek koncových uživatelů, kteří by testovali chyby v pilotním režimu	Pracovníci jsou příliš vytížení svou prací, pilotní režim testují v přesčasových hodinách apod.	Prodloužení doby pilotního režimu	Finanční ohodnocení za pomoc při řešení chyb v pilotním režimu	2	3	1	6	Nasazení	Vedení banky zajistí dostatečný počet pracovníků, jejichž hlavní náplní práce bude testování pilotního režimu IS	1	3	1	3
		Nedostatečné proškolení uživatelů	Nepřipravenost team leadrů a školitele, nekvalitně zpracovaná dokumentace k IS	Uživatel není schopen v IS pracovat, prodlužuje se doba odbavení klienta, zvýšené hlášení chybových požadavků na helpdesk	Zajištění dostatečného množství testovacích PC a školení, feedback ke školení	3	4	4	48	Provoz	Kontrola připravené dokumentace	2	4	4	32
	Definování krizových scénářů	Neodhadnutí nebo chybné nastavení minimální konfigurace	Chyba helpdesku	Zpomalení zpracování procesů a systémů	Kontrola konfigurace, výměna HW	1	4	1	4	Nasazení	Stanovení přesných požadavků na jednotlivé programy	1	5	1	5
		Nedostatečné testování v pilotním režimu	Zadavatel chce urychlit proces nasazení IS	Chyby v ostrém provozu, nezajištění plynulého provozu	Časová rezerva pro testování v pilotním režimu	1	5	1	5	Nasazení	Stejná jako současná	1	5	1	5
		Nedefinování všech krizových scénářů	Opomenutí některého krizového scénáře projektovým týmem nebo přijetí rizika	Scénář nemusí nastat, a pokud ano, dojde k roll-backu	Kontrola krizových scénářů více lidmi	1	5	1	5	Nasazení	Stejná jako současná	1	5	1	5
	Odstávka	Nedodržení harmonogramu odstávky	Technické problémy v migraci, chyba týmu	Roll-back systému	Časová rezerva v harmonogramu odstávky	2	5	1	10	Nasazení	Nasazovací tým rozšířit o více zkušených expertů	1	5	1	5
		Nedodržení postupu nasazení	Chyba realase managera	Prodloužení odstávky, klienti nemají přístup na své účty, roll-back systému	Zhotovení podrobného harmonogramu při nasazení, kontrola jednotlivých kroků v harmonogramu, kontrola více llidmi	1	5	1	5	Nasazení	Stejná jako současná	1	5	1	5
		Neodhalení chyb ve smoke testu	Chyba testera nebo kohokoliv z projekčního týmu	Nedodržení harmonogramu odstávky	Test provádí tester senior, zajištění dostatku času na testování během odstávky	1	4	1	4	Nasazení	Podrobná definice testovacích scénářů smoke testu	1	4	1	4
		Nezálohování původního stavu systému	Chyba nasazovacího týmu	Ztráta funkční konfigurace IS, úplná ztráta dat, ztráta posledních nových funkčností, dostupná pouze nefunkční verze	Dvojí kontrola zálohování	1	5	3	15	Nasazení	Kontrola realase managerem	1	5	2	10
	Provoz	Uživatelé nejsou schopni pracovat v novém IS	Nasazení špatné verze IS, která je nekompatibilní se systémy, které byly nasazeny s danou verzí IS, chyba dodavatele balíků (nasazovací tým)	Uživatel nemůže odbavit klienta po telefonu ani provádět aktivní operace na účtu	Kontrola dodávaných balíků a verzí IS	2	5	1	10	Provoz	Kontrola nasazované verze realase managerem	1	5	1	5
		Výpadek některých systémů, které jsou kritické pro funkčnost IS	Přetížení systému, odstávka elektřiny, zhroucení některého systému	Neplynulý provoz, pomalejší, nebo žádné odbavení klienta	Celý projektový tým je seznámen s krizovými plány a zajistí jejich dodržení	1	5	1	5	Provoz	Popsání krizových plánů v dokumentaci pro potřeby projektového týmu a uživatelů IS	1	5	1	5

Příloha č. 9 – FMECA: Odstranění chyb

Proces	Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	Současná opatření	O	S	D	RPN	Fáze odhalení	Doporučené opatření	O	S	D	RPN
ODSTRANĚNÍ CHYB	Neodstraní se všechny chyby	Chyba vývojářů nebo tlak na urychlení procesu nasazení	Nefunkčnost některých systémů	Nelze zajistit stoprocentní opatření	3	4	1	12	Odstranění chyb / Provoz	Prodloužení doby testů	2	4	1	8
	Odstraněná chyba způsobí další chybu	Vývojář neopraví všechny chyby které se vyskytnou po změně kódu, nebo systémová analýza obsahuje nedostatky	Neplynulý provoz, ztížení některých procesů, nedostatečná funkčnost	Průběžné opravy chyb, dodatečná kontrola kódů vývojářem	2	4	1	8	Odstranění chyb / Provoz	Prodloužení doby testů, vývojář získá více času na opravu chyb	1	4	1	4
	Chybám se neuděluje priorita (nebo nerelavantní priorita)	Uživatel si neuvědomuje rozsah chyb	Odstraňování chyb ve špatném pořadí	Uživatelská podpora stanoví priorizaci chyb při výskytu chyby	4	4	2	32	Odstranění chyb / Provoz	Kvalitnější proškolení uživatelů, informovanost uživatelů o dopadů neopravených chyb na systém	2	4	2	16

Příloha č. 10 – FMECA: Akceptace projektu

Proces	Identifikované nebezpečí	Potenciální příčina poruchy	Potenciální následek poruchy	Současná opatření	O	S	D	RPN	Fáze odhalení	Doporučené opatření	O	S	D	RPN
AKCEPTACE PROJEKTU	Dokumentace k IS je nepřehledná nebo neúplná	Zadavatel nedostatečně specifikuje požadavky na dokumentaci, nebo zhotovitel opomene některé z těchto požadavků	Prodloužení doby při řešení problémů popsaných v dokumentaci, nutnost další komunikace s dodavatelem	Před akceptací dokumentaci k IS ji zkontroluje projekční tým zadavatele	3	5	1	15	Provoz	Dokumentaci k IS zkontrolují kromě projekčního týmu i vybraní koncoví uživatelé IS	2	5	1	10
	Zhotovitel neposkytuje dostatečnou technickou podporu pracovníkům projektu zadavatele	Smlouva neobsahuje všechny náležitosti, zejména dodatek o technické a uživatelské podpoře, nebo zhotovitel nedodržuje smluvní podmínky	Bez technické podpory zhotovitele IS je vytváření nových funkčností složité a zdlouhavé	Kontrola business zadavatele, že smlouva obsahuje všechny náležitosti	2	5	1	10	Akceptace	Smlouva by měla být zhotovena podle metodiky Information Technology Infrastructure Library, záruky v SLA by měly být měřitelné, SLA by měl být doplněn o Operational Level Agreement	1	5	1	5
	Zhotovitel nedodá všechny požadované protokoly pro funkčnost IS zadavateli, nebo jsou tyto protokoly neúplné	Chyba na straně zhotovitele	Chyby ve funkčnostech IS	Ošetření Service Level Agreement, ve kterém jsou stanoveny postihy v případě nedodržení smluvních podmínek	2	5	1	10	Akceptace	Zohlednění referencí na zhotovitele IS při výběrovém řízení, výběr důvěryhodného zhotovitele	1	5	1	5
	Zadavatel má k projektu výhrady a projekt nechce akceptovat	IS neodpovídá představám zadavatele, příčina může být ve kterékoliv části procesu	Pokud zhotovitel vytvořil a implementoval IS podle požadavků zadavatele a podle Service Level Agreement, zadavatel projekt musí akceptovat a doplatit zbývající částku za projekt	Průběžná kontrola požadavků na IS ve všech částech procesu zadavatelem	4	5	1	20	Akceptace	Dostatečná časová rezerva pro klíčové fáze procesu, zejména pro fáze stanovení požadavků, vytváření návrhu a implementace. Snaha o vyjasnění si všech požadavků v obou směrech a zapojení dostatečného množství koncových uživatelů IS na stanovování těchto požadavků	3	5	1	15